

RÁMCOVÁ DOHODA na zajištění penetračních testů a bezpečnostních prověrek integrovaného informačního systému ČSSZ

uzavřená níže uvedeného dne, měsíce a roku dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v platném a účinném znění (dále jen „**Občanský zákoník**“),
mezi níže uvedenými stranami

(dále jen „**Smlouva**“)

Česká republika – Česká správa sociálního zabezpečení

Sídlo: Křížová 25, 225 08 Praha 5
Statutární zástupce: Mgr. Pavel Krejčí, pověřen zastupováním ústředního ředitele ČSSZ
Jednající: Ing. Milan Shrbený, ředitel sekce informačních a komunikačních technologií
IČO: 00006963
DIČ: neplátce
Bankovní spojení: Česká národní banka
Číslo účtu: 10006-127001/0710
ID datové schránky: 49kaiq3

(dále jen „**Objednatel**“)

na straně jedné

a

KPMG Česká republika, s.r.o.

Sídlo: Pobřežní 648/1a, 186 00 Praha 8
Zastoupená: [REDACTED] prokuristou se samostatnou prokurou
Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 326
IČO: 00553115
DIČ: CZ699001996
Bankovní spojení: Česká spořitelna, a.s.
Číslo účtu: 2518612/0800
ID datové schránky: hbcgtsz

(dále jen „**Poskytovatel**“)

na straně druhé

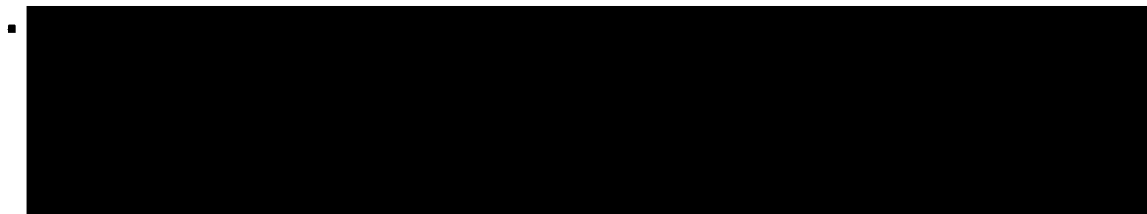
(Objednatel a Poskytovatel dále také společně označování jako „**Smluvní strany**“ nebo jednotlivě jako „**Smluvní strana**“)



Preambule

1. Objednatel prohlašuje, že

- je organizační složkou státu a správním orgánem, který zabezpečuje výběr pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, dále provádí zejména důchodové pojištění a zajišťuje agendu nemocenského pojištění;



- splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

2. Poskytovatel prohlašuje, že

- je podnikatelem dle ustanovení § 420 a násl. Občanského zákoníku;
- splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené;
- je odborníkem v oblasti poskytování služeb dle této Smlouvy a bude své povinnosti plnit s náležitou a odbornou péčí.

3. Tato Smlouva se uzavírá za účelem zajištění služeb pro Objednatele v oblasti penetračního testování v rozsahu a za podmínek uvedených dále v této Smlouvě.

I. Předmět Smlouvy

1. Předmětem této Smlouvy je stanovení podmínek, za kterých se Poskytovatel zavazuje poskytovat Objednateli služby spočívající v penetračním testování a bezpečnostních prověrkách infrastruktury prvků integrovaného informačního systému ČSSZ Objednatele (dále jen „**IIS ČSSZ**“), a to na základě a v souladu s dílčími objednávkami případně dílčími smlouvami uzavíranými postupem dle čl. IV., Přílohy č. 7 a v souladu s dalšími případnými pokyny Objednatele (dále jen „**Předmět plnění**“).
2. Předmět plnění sestává z penetračního testování pro integrační, testovací a produkční prostředí IIS ČSSZ minimálně v rozsahu aktuální verze OWASP Top 10 dle Open Web Application Security Project, dle níže uvedených okruhů:
 - A. Externí penetrační testování - prvotní externí penetrační testování
 - B. Externí penetrační testování - následné externí penetrační testování
 - C. Interní penetrační testování – prvotní interní penetrační testování
 - D. Interní penetrační testování - následné interní penetrační testování
 - E. Bezpečnostní prověrka infrastruktury prvků IIS ČSSZ
 - F. Vyhotovení Závěrečné zprávy z provedení penetračního testování nebo bezpečnostní prověrky
 - G. Konzultační činnost bezpečnostního specialisty Poskytovatele uvedeného v Příloze č. 6 Smlouvy (dále jen „**Bezpečnostní specialista**“) k Závěrečné zprávě a při realizaci doporučení vyplývajících ze Závěrečné zprávy, („**Okruhy**“ a každý samostatně jako „**Okruh**“).

3. Vždy po ukončení testování Okruhu a/nebo (dle volby Objednatele) po dokončení všech Okruhů bude Poskytovatelem vyhotovena Závěrečná zpráva z penetračních testů, nebo Závěrečná zpráva o provedení bezpečnostní prověrky (dále jen „**Závěrečná zpráva**“). Závěrečná zpráva bude Poskytovatelem předložena Objednateli vždy po ukončení Okruhu nebo všech Okruhů výhradně osobě oprávněné jednat ve věcech věcného plnění Objednatele, přičemž Závěrečná zpráva bude vždy obsahovat alespoň:
- manažerské shrnutí tzn. přehled hlavních zjištění a doporučení, časový rámec testu, cíl a rozsah testů, způsob připojení apod. U dobře známých a jednoduše prokazatelných zranitelností bude uveden i postup zneužití dané zranitelnosti,
 - shrnutí známých informací o testované aplikaci, které byly získány z testování a jsou tedy dostupné potenciálnímu útočníkovi,
 - detailní postup při provádění penetračních testů včetně použitých nástrojů a technik,
 - přehled testovaných zranitelností v souladu s OWASP Testing Guide v4 s kapitolou Reporting,
 - přehledný seznam identifikovaných zranitelností, seřazený sestupně podle jejich závažnosti a jejich popis, kdy bude použito jednotné klasifikační schéma (např. klasifikační schéma DREAD- „*damage, reproducibility, exploitability, affected users, discoverability*“),
 - doporučený postup předcházení uvedeným zranitelnostem, pokud takový existuje, případně popis vhodných alternativních protipatření.

V případě Závěrečné zprávy o provedení bezpečnostní prověrky infrastruktury

- identifikované zranitelnosti klíčových prvků,
 - doporučení na zmírnění rizika zneužití identifikovaných zranitelností,
 - hodnocení úrovně bezpečnosti a hodnocení rizik.
4. Před zasláním Závěrečné zprávy je Poskytovatel povinen předložit Objednateli předběžnou zprávu, která bude obsahovat předběžný a stručný (manažerský) souhrn informací, které mají být součástí Závěrečné zprávy (dále jen „**Předběžná zpráva**“) v následujících lhůtách:
- a) do 24 (slovy: čtyřicet) hodin od okamžiku skončení testování Okruhu a/nebo (dle volby Objednatele) po dokončení všech Okruhů v případě, že bude Poskytovatelem při testování zjištěna jakákoliv závažná zranitelnost IIS ČSSZ nebo jeho subsystému, přičemž v takovém případě je Poskytovatel současně povinen neprodleně po zjištění o povaze zjištěné zranitelnosti alespoň stručně informovat Objednatele prostřednictvím e-mailu či telefonu osoby oprávněné jednat za Objednatele ve věcech věcného plnění,
 - b) do 2 (slovy: dvou) pracovních dnů ode dne skončení testování Okruhu a/nebo (dle volby Objednatele) po dokončení všech Okruhů v případě, že nebude Poskytovatelem při testování zjištěna žádná závažná zranitelnost IIS ČSSZ nebo jeho subsystému.
5. Jednotlivé Okruhy jsou blíže specifikovány v Příloze č. 1 této Smlouvy.
6. Objednatel předpokládá, že za dobu trvání této Smlouvy bude provedeno přibližně 48 (slovy: čtyřicet) penetračních testů a 4 (slovy: čtyři) bezpečnostní prověrky infrastruktury prvků IIS ČSSZ. Tento počet je však pouze orientační, přičemž konkrétní počet bude záviset na průběhu čerpání rozsahu člověkohodin na základě Dílčích smluv (jak je tento pojem definován níže).

7. Objednatel poskytne pracovníkům Poskytovatele po dobu poskytování Předmětu plnění přístup do prvků IIS ČSSZ z konkrétních IP adres Poskytovatele, které Poskytovatel Objednateli uvedl v Příloze č. 1 v části věnované součinnosti Poskytovatele; nelze-li objektivně takové IP adresy uvést dopředu, oznámí Poskytovatel takové IP adresy Objednateli alespoň 4 (slovy: čtyři) pracovní dny před zahájením plnění Dílčí smlouvy (jak je tento pojem definován níže) prostřednictvím autorizačního dopisu, jehož vzor tvoří Přílohu č. 8 (dále jen „**Autorizační dopis**“).
8. Předmětem této Smlouvy je dále stanovení podmínek, za kterých se Objednatel zavazuje platit za Předmět plnění Poskytovateli dohodnutou cenu na základě a v souladu s podmínkami uvedenými v čl. V. této Smlouvy.

II. Výklad pojmů

1. Externími penetračními testy se rozumí testy, které budou simulovat napadení útočníkem, který má pouze veřejně dostupné informace. Tyto testy budou zaměřeny na aplikace vnějšího webového rozhraní IIS ČSSZ.
2. Interními penetračními testy se rozumí testy, které budou prováděny z vnitřní části sítě Objednatele s cílem detekovat zranitelnosti, které mohou vést k získání neoprávněných informací nebo k získání přístupu k jednotlivým systémům IIS ČSSZ.
3. Prvotními penetračními testy se rozumí takové testování, kdy není Poskytovateli vůbec známa struktura testované aplikace IIS ČSSZ a neprováděl v minulosti žádné penetrační testování na této aplikaci. Cílem prvotních penetračních testů je odhalit co největší množství zranitelností v testované aplikaci IIS ČSSZ, odhalit způsob jejich využití a případnou možnost získání neoprávněných přístupů. Za prvotní penetrační testy jsou považovány i testy, které jsou prováděny po významných změnách v testované aplikaci anebo IIS ČSSZ.
4. Následnými penetračními testy se rozumí takové testování, které následuje po odstranění dříve nalezených zranitelností. Hlavním cílem je potvrdit nebo vyvrátit, že dříve nalezená zranitelnost byla odstraněna.
5. Bezpečnostní prověrka infrastruktury prvků IIS ČSSZ posoudí stávající IIS ČSSZ z pohledu bezpečnosti a doporučí odpovídající nastavení jednotlivých systémů a prvků IIS ČSSZ tak, aby byla v souladu s doporučením výrobců a předních organizací, které se zabývají bezpečností informací a zabezpečením informačních systémů (např. IEF, CVE, apod.).
6. Závažná zranitelnost je zranitelnost, jejímž zneužitím může dojít k vážnému poškození IIS ČSSZ nebo souvisejícího testovaného systému či aplikace Objednatele.
7. Bezpečnostní specialista, který je ve smluvním vztahu se Poskytovatelem, je schopen provést penetrační testování a bezpečnostní prověrku infrastruktury. Nalezených zranitelností je schopen využít, ale také navrhnout vhodná opatření a je informován o nejnovějších hrozbách a zranitelnostech.

III. Doba a místo plnění

1. Poskytovatel zahájí poskytování Předmětu plnění Objednateli počínaje dnem nabytí účinnosti první z Dílčích smluv uzavřených na základě této Smlouvy a bude ho poskytovat po dobu trvání této Smlouvy, resp. jednotlivých Dílčích smluv, a to tak, jak je uvedeno v čl. IV. této Smlouvy.
2. Místem plnění této Smlouvy je sídlo Objednatele na adrese Křížová 25, 225 08 Praha 5 a Trojská 13a, 182 00 Praha 8.

IV. Způsob realizace a předání Předmětu plnění

1. Objednatel zpravidla určí (zadá) Poskytovateli do 20. (slovy: dvacátého) dne předchozího kalendářního měsíce na následující kalendářní měsíc objednávku definující konkrétní Okruh, konkrétní termín pro jeho splnění, maximální počet člověkohodin vyhrazený pro toto plnění a další případné doplňující podmínky (pokyny Objednatele) k provedení Okruhu. Podrobný popis postupu uzavírání Dílčích smluv je uveden v Příloze č. 7. Dnem potvrzení objednávky, dnem marného uplynutí lhůty pro potvrzení objednávky či vyjádření nesouhlasu s objednávkou, nebo dnem doručení určení maximálního počtu člověkohodin a termínu plnění Objednatel Poskytovateli, podle toho, který okamžik nastane dříve, dochází k uzavření dílčí smlouvy na plnění konkrétního Okruhu, za podmínek stanovených touto Smlouvou a v objednávce (dále jen „**Dílčí smlouva**“). Součástí každé Dílčí smlouvy jsou podmínky stanovené v této Smlouvě.
2. Splnění Dílčí smlouvy se Poskyvatel zavazuje doložit Výkazem plnění (dále jen „**Výkaz**“), jehož vzor tvoří Přílohu č. 3 této Smlouvy, přičemž tento Výkaz bude vypracován a podepsán Poskytovatelem a doručen Objednateli vždy po dokončení plnění Dílčí smlouvy v souladu s termíny dle tohoto článku odstavce 3 této Smlouvy. Přílohou Výkazu bude vždy také Závěrečná zpráva dle čl. I. odst. 3. této Smlouvy. Předložení Výkazu nezabývá Poskytovatele povinností zpracovat a předložit Závěrečnou zprávu.
3. Poskytovatel je povinen předložit Objednateli (i) Závěrečnou zprávu k akceptaci do 5 (slovy: pěti) pracovních dnů ode dne akceptace Předběžné zprávy Objednatel a (ii) Výkaz k akceptaci do 5 (slovy: pěti) pracovních dnů ode dne akceptace Závěrečné zprávy Objednatel.
4. V případě, že Výkaz (včetně jeho příloh) nebude mít dle názoru Objednatele odpovídající náležitosti stanovené touto Smlouvou, náležitosti specifikované v Dílčí smlouvě, další náležitosti obvyklé u takového Výkazu, bude mít jiné nedostatky anebo bude obsahovat vady/chyby (jak gramatické, tak metodické, tj. kvalitativní obsahové), je Objednatel oprávněn Výkaz vrátit zpět Poskytovateli k doplnění či opravě (neakceptovat), přičemž Poskytovatel je v takovém případě povinen předložit opravený Výkaz opětovně Objednateli k akceptaci do 3 (slovy: tří) pracovních dnů ode dne jeho vrácení Objednatel, přičemž takové vrácení může probíhat opakovaně do doby úplného odstranění nedostatků Výkazu. Je-li pro vypracování bezvadného Výkazu nezbytné provést některé činnosti opakovaně, zavazuje se Poskytovatel takové činnosti provést na vlastní náklady (bezúplatně) tak, aby byl bezvadný Výkaz předložen Objednateli včas. Ustanovení tohoto článku tohoto odstavce této Smlouvy se užije obdobně na Závěrečnou zprávu a Předběžnou zprávu; v případě akceptace Předběžné zprávy dle článku I. odst. 4 písm. a) této Smlouvy se lhůty stanovené v tomto článku tohoto odstavce této Smlouvy zkracují na polovinu.
5. Objednatel je oprávněn v zadání dle odst. 1 tohoto článku této Smlouvy nebo následně při plnění Dílčí smlouvy požadovat, aby Objednatel určená osoba byla přítomna některých nebo všech činností prováděných v rámci plnění Dílčí smlouvy a mohla tak kontrolovat průběh jejího plnění a seznamovat se s postupy plnění této Smlouvy a jednotlivých Dílčích smluv. Poskytovatel se zavazuje kontrolu plnění Dílčí smlouvy alespoň v rozsahu dle tohoto odstavce tohoto článku této Smlouvy umožnit, poskytovat informace Objednatel určené osobě, poskytovat veškerou možnou součinnost k provedení kontroly a zajistit efektivní výkon takové kontroly.
6. Akceptací, tj. podpisem předloženého Výkazu Objednatel, Objednatel rozsah i kvalitu plnění dle Dílčí smlouvy uznává, takové plnění se považuje za dokončené a Objednatel se zavazuje k zaplacení ceny za takto poskytnuté plnění Dílčí smlouvy. Až akceptací Výkazu včetně Závěrečné zprávy vzniká Poskytovateli právo na zaplacení ceny za příslušné plnění. Akceptací Výkazu nejsou dotčena práva Objednatele z vadného plnění.

7. Objednatel není povinen zasílat žádné objednávky a není povinen uzavřít žádnou Dílčí smlouvu. Součástí plnění Dílčí smlouvy (tj. povinnostmi Poskytovatele) jsou veškeré činnosti, které je nezbytné provést tak, aby došlo testování anebo prověrce všech rizik, a to alespoň v rozsahu a kvalitě dle OWASP Top 10 a této Smlouvy včetně jejích příloh a bylo možné vypracovat Závěrečnou zprávu alespoň v rozsahu a kvalitě dle OWASP Testing Guide v4 Open Web Application Security Project a dle této Smlouvy včetně jejích příloh.

V. Cena a platební podmínky

1. Celková cena za poskytnutí Předmětu plnění v maximálním rozsahu 4 900 člověkohodin činí **4 067 000,- Kč (slovy: čtyři miliony šedesát sedm tisíc korun českých) bez DPH, tedy 4 921 070,- Kč (slovy: čtyři miliony devět set dvacet jedna tisíc sedmdesát korun českých) včetně DPH, výše DPH činí 854 070,- Kč (slovy: osm set padesát čtyři tisíc sedmdesát korun českých)**, (dále jen „Cena“).
2. Bližší specifikace Ceny je uvedena v Příloze č. 2 této Smlouvy.
3. Ceny uvedené v Příloze č. 2 této Smlouvy jsou cenami nejvýše přípustnými a závaznými po celou dobu trvání této Smlouvy. Ceny včetně daně z přidané hodnoty uvedené v Příloze č. 2 této Smlouvy mohou být překročeny pouze v souvislosti se změnou daně z přidané hodnoty mající prokazatelný vliv na Cenu, a to pouze o výši, která této změně bude odpovídat. Z jakýchkoliv jiných důvodů nesmí být ceny v Příloze č. 2 a tudíž ani Cena překročeny.
4. Cena obsahuje veškeré náklady Poskytovatele související s poskytnutím Předmětu plnění dle této Smlouvy, včetně případných nákladů nebo souvisejících výdajů spojených s případnou přítomností Bezpečnostního specialisty anebo členů realizačního týmu v sídle Objednatele.
5. Platba za plnění dle Dílčí smlouvy bude Objednatelem provedena na základě daňového dokladu (faktury) vystaveného Poskytovatelem do 10. (slovy: desátého) dne měsíce následujícího po měsíci, v němž bylo plnění dle Dílčí smlouvy akceptováno Objednatelem znějící na počet skutečně efektivně strávených člověkohodin na plnění takové Dílčí smlouvy (do výše maximálního počtu člověkohodin sjednaného v takové Dílčí smlouvě), vynásobený cenou za jednu člověkohodinu dle této Smlouvy. Nedílnou součástí daňového dokladu (faktury) bude vždy oběma Smluvními stranami podepsaný Výkaz ve struktuře dle Přílohy č. 3 této Smlouvy. Dnem zdanitelného plnění je v takovém případě den, kdy bylo plnění konkrétní Dílčí smlouvy Objednatelem akceptováno.
6. Splatnost řádně vystaveného daňového dokladu (faktury) činí 30 (slovy: třicet) kalendářních dní ode dne jeho doručení Objednateli.
7. Daňový doklad (faktura) musí obsahovat náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dle této Smlouvy. V případě, že daňový doklad (faktura) nebude mít odpovídající náležitosti nebo bude jinak v rozporu s touto Smlouvou či Dílčí smlouvou, je Objednatel oprávněn daňový doklad (fakturu) zaslat ve lhůtě splatnosti zpět Poskytovateli k doplnění či opravě, a to i opakovaně, aniž se tak dostane do prodlení s úhradou oprávněně fakturované ceny; lhůta splatnosti počíná běžet znovu ode dne doručení náležitě doplněného či opraveného daňového dokladu (faktury) Objednateli.
8. Není-li Poskytovatel registrovaným plátcem DPH při podpisu této Smlouvy, potom tuto daň nevyčíslí. Skutečnost, že není plátcem DPH, bude uvedena v hlavičce této Smlouvy. Smluvní strany berou na vědomí, že pokud se Poskytovatel stane plátcem DPH až po uzavření této Smlouvy, platí, že ceny uvedené v této Smlouvě v sobě již DPH zahrnovaly. Poskytovatel je tedy povinen příslušnou část celkové ceny Předmětu plnění odvést jako DPH a nemá vůči Nabyvateli z titulu DPH nárok na další plnění nad rámec celkové ceny Předmětu plnění.

9. Cena nebo její část bude vždy hrazena bezhotovostním převodem z účtu Objednatele na účet Poskytovatele uvedený v záhlaví této Smlouvy. Platby budou probíhat výhradně v české měně (CZK) a rovněž veškeré cenové údaje budou uvedeny v této měně.
10. Platba se považuje za uhrazenou okamžikem odepsání odpovídající částky z účtu Objednatele.
11. Objednatel neposkytuje Poskytovateli jakékoliv zálohy na Cenu nebo její část.

VI. Další práva a povinnosti Smluvních stran

1. Poskytovatel se zavazuje, že bude Předmět plnění poskytovat řádně, s odbornou péčí, v ujednaném čase, v ujednané kvalitě, v souladu s touto Smlouvou, Dílčími smlouvami a v souladu s obecně závaznými právními předpisy platnými a účinnými v době poskytování Předmětu plnění a dle pokynů Objednatele.
2. V případě rozporu ustanovení Dílčí smlouvy s touto Smlouvou, mají pro plnění příslušné Dílčí smlouvy přednost ustanovení takové Dílčí smlouvy.
3. Poskytovatel se zavazuje, že bude při poskytování Předmětu plnění úzce spolupracovat s Objednatelem a konzultovat veškeré zásadní nebo problematické otázky (např. součinnost s pracovníky Objednatele, prodlení na straně operátorů datového připojení), a dále, že bude bez zbytečného prodlení informovat Objednatele o vzniklých skutečnostech ovlivňujících poskytování Předmětu plnění.
4. Poskytovatel nemůže nad rámec Předmětu plnění jakýmkoli způsobem vstupovat do informačních systémů Objednatele bez jeho výslovného souhlasu, ani se o to pokoušet či vyvíjet jakoukoliv jinou činnost, kterou by byl nebo mohl být ohrožen, narušen nebo znemožněn provoz Objednatele, neudělí-li k takové činnosti Objednatel výslovný souhlas.
5. Poskytovatel se zavazuje, že bude při poskytování Předmětu plnění dodržovat aktuálně platné standardy IKT Objednatele, se kterými byl Poskytovatel seznámen, a jejichž seznam je uveden v Příloze č. 4 této Smlouvy.
6. Objednatel je povinen poskytnout Poskytovateli nezbytnou součinnost k plnění povinností Poskytovatele z této Smlouvy nebo Dílčích smluv. Požadavek na součinnost Objednatele se Poskytovatel zavazuje sdělit Objednateli vždy alespoň 5 (slovy: pět) pracovních dnů předem, přičemž součinnost Objednatele za celý Předmět plnění nepřekročí 160 člověkohodin a součinnost bude poskytována vždy v obvyklé pracovní době Objednatele, nedohodnou-li se Smluvní strany jinak. Objednatel je oprávněn součinnost odmítnout, pokud by její poskytnutí závažně narušilo jeho běžnou činnost.
7. Poskytovatel se zavazuje na žádost Objednatele a v termínu v žádosti uvedeném, který nebude kratší než 2 (slovy: dva) pracovní dny, zajistit přítomnost Bezpečnostního specialisty anebo členů realizačního týmu v sídle Objednatele nebo na jiném místě uvedeném Objednatelem v žádosti dle tohoto článku tohoto odstavce této Smlouvy.

VII. Sankční ujednání a náhrada škody

1. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty za prodlení Poskytovatele s předložením Předběžné zprávy k akceptaci oproti termínu dohodnutému v čl. I. odst. 4. písm. a) této Smlouvy ve výši 2.000,- Kč (slovy: dva tisíce korun českých) za každou i započatou hodinu prodlení.
2. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty za prodlení Poskytovatele s předložením Předběžné zprávy k akceptaci oproti termínu dohodnutému v čl. I.

odst. 4. písm. b) této Smlouvy ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení.

3. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty za prodlení Poskytovatele s předložením Výkazu anebo Závěrečné zprávy k akceptaci oproti termínu dohodnutému v čl. IV. odst. 3. této Smlouvy ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení.
4. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty v případě nedodržení lhůty pro přijetí objednávky nebo vyjádření nesouhlasu (tj. včetně přijetí návrhu, zaslání oponentního návrhu, nesouhlasu atd.), tj. porušení povinnosti zaslat příslušnou odpověď ve stanovených lhůtách, dle čl. IV. odst. 1. a Přílohy č. 7 této Smlouvy ve výši 20.000,- Kč (slovy: dvacet tisíc korun českých) za každý takový případ porušení povinnosti.
5. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty za prodlení Poskytovatele s opětovným předložením opraveného Výkazu anebo Závěrečné zprávy k akceptaci oproti termínu dohodnutému v čl. IV. odst. 4. této Smlouvy ve výši 2.000,- Kč (slovy: dva tisíce korun českých) za každý i započatý den prodlení.
6. Objednatel je oprávněn požadovat na Poskytovateli zaplacení smluvní pokuty za prodlení Poskytovatele s plněním Dílčí smlouvy ve výši 0,05 % z částky vypočítané jako cena za jeden člověkodenní dle Přílohy č. 2 Smlouvy vynásobená maximálním počtem člověkodenní dle Dílčí smlouvy, a to za každý i započatý den prodlení.
7. Poskytovatel se zavazuje v případě porušení kteréhokoliv ze závazků uvedených v čl. IX. odst. 6, 7, 8, 9, 12, 14, 15, 16, 17 a 19 této Smlouvy zaplatit Objednateli smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých) za každé takové porušení.
8. Poskytovatel se zavazuje v případě porušení závazku uvedeného v čl. VI. odst. 4. této Smlouvy zaplatit Objednateli smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých) za každé takové porušení.
9. Uplatněním smluvní pokuty není dotčeno právo Objednatele na náhradu újmy způsobené porušením povinnosti, na kterou se smluvní pokuta vztahuje, v plném rozsahu ani povinnost Poskytovatele uhradit Objednateli jakoukoliv sankci, která bude uložena Objednateli v důsledku jednání Poskytovatele.
10. Smluvní pokuty mohou být libovolně kombinovány, tzn. uplatnění jedné smluvní pokuty, nevylučuje souběžné uplatnění jakékoliv jiné smluvní pokuty.
11. Smluvní pokuta je splatná do 30 (slovy: třiceti) dnů ode dne doručení oznámení o uložení smluvní pokuty Poskytovateli. V případě prodlení s úhradou smluvní pokuty uhradí Poskytovatel Objednateli úrok z prodlení podle nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob, v platném a účinném znění (dále jen „**Nařízení**“).
12. V případě prodlení s úhradou oprávněně vystaveného daňového dokladu (faktury) uhradí Objednatel Poskytovateli z nezaplacené částky úrok z prodlení ve výši určené Nařízením.
13. Poskytovatel se zavazuje, že bude mít po celou dobu trvání smluvního vztahu sjednáno pojištění odpovědnosti za škodu způsobenou Objednateli nebo třetí osobě při výkonu podnikatelské činnosti na základě této Smlouvy anebo jakékoliv Dílčí smlouvy s limitem pojistného plnění ve výši nejméně 10.000.000,- Kč (slovy: deset milionů korun českých) za rok, přičemž spoluúčast



Poskytovatele nebude vyšší než 5 % (pět procent) z limitu pojistného plnění. Tuto skutečnost je Poskytovatel povinen prokázat kdykoliv po dobu trvání této Smlouvy k výzvě Objednatele tím, že doručí a předá Objednateli pojistnou smlouvu (originál či úředně ověřenou kopii) či podobný doklad o trvání pojištění (pojistku) do 7 (sedmi) kalendářních dnů od doručení této výzvy. Porušení této povinnosti bude považováno za podstatné porušení Smlouvy. Poskytovatel předložil Objednateli před podpisem této Smlouvy doklad o uzavření pojištění dle tohoto odstavce tohoto článku Smlouvy.

VIII. Odpovědnost za újmu

1. Objednatel je oprávněn požadovat na Poskytovateli a Poskytovatel je povinen poskytnout Objednateli náhradu újmy, kterou Poskytovatel způsobil Objednateli porušením povinností daných touto Smlouvou, Dílčími smlouvami nebo v souvislosti s plněním této Smlouvy, včetně případů, kdy se jedná o takové porušení povinností dané touto Smlouvou, na které se vztahuje smluvní pokuta. Jakékoliv omezení výše či druhu náhrady újmy není přípustné. Újma se hradí v penězích, případně uvedením do předešlého stavu podle volby Objednatele v každém konkrétním případě.
2. Poskytovatel se zavazuje poskytnout Předmět plnění specifikovaný v této Smlouvě řádně a včas bez faktických a právních vad.
3. Objednatel je oprávněn domáhat se náhrady újmy v plné výši, přičemž škodou se rozumí skutečná škoda a ušlý zisk a dále náklady, které musel Objednatel vynaložit v důsledku porušení povinností Poskytovatele.

IX. Ochrana informací

1. Poskytovatel se zavazuje, že neužije informace získané v souvislosti s plněním této Smlouvy jinak než pro účely plnění této Smlouvy a Dílčích smluv a v souladu s účelem, pro který byly takové informace získány.

Předmět zpracování, kategorie subjektů údajů a typ osobních údajů

2. S ohledem na předmět této Smlouvy smluvní strany nemohou vyloučit, že Poskytovatel bude zpracovávat osobní údaje nebo zvláštní kategorie osobních údajů (citlivé údaje) (dále společně jen „**osobní údaje**“) obsažené v informačních systémech Objednatele či osob evidovaných v informačních systémech Objednatele (dále jen „**koncoví uživatelé**“). Nedílnou součástí Smlouvy je tak i ujednání o zpracování osobních údajů mezi Objednatелеm jako správcem a Poskytovatelem jako zpracovatelem, uvedené níže v tomto čl. IX. této Smlouvy.
3. Podrobněji jsou předmět zpracování, kategorie subjektů údajů, typ osobních údajů a rozsah zpracování osobních údajů popsány v této Smlouvě.

Povaha, účel a prostředky zpracování

4. Poskytovatel nezpracovává osobní údaje automatizovanými prostředky za účelem plnění této Smlouvy. Podrobněji jsou povaha, účel a prostředky zpracování osobních údajů popsány v této Smlouvě.

Doba zpracování

5. Zpracování osobních údajů bude ze strany Poskytovatele probíhat po dobu účinnosti této Smlouvy. Povinnosti Poskytovatele týkající se ochrany osobních údajů se Poskytovatel zavazuje plnit po celou dobu účinnosti Smlouvy, pokud z ustanovení Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti.

Obecné zásady zpracování osobních údajů

6. Poskytovatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli vyplývají z právních předpisů o ochraně osobních údajů, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.
7. Poskytovatel v souvislosti se zpracováním osobních údajů:
 - a) zpracovává osobní údaje výlučně na základě pokynů Objednatele učiněných v souladu se zásadami komunikace dle této Smlouvy, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo členského státu, které se na Objednatele vztahuje; v takovém případě Poskytovatel Objednatele informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
 - b) v případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Poskytovatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Poskytovatelem, oznámí tuto skutečnost okamžitě Objednateli a poskytne mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení;
 - c) poskytne Objednateli součinnost při komunikaci s dozorovým orgánem a dle pokynů Objednatele bude spolupracovat při přípravě odpovědí dozorovému úřadu ohledně činností prováděných Poskytovatelem;
 - d) nezpracovává osobní údaje získané za účelem plnění této Smlouvy pro své vlastní účely;
 - e) nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele;
 - f) zohledňuje povahu zpracování,
 - g) je Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Objednatelovy povinnosti reagovat na žádosti o výkon práv koncových uživatelů;
 - h) je Objednateli nápomocen při zajišťování souladu s povinnostmi Objednatele zajistit úroveň zabezpečení zpracování a ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu a případně též koncovým uživatelům, posuzovat vliv na ochranu osobních údajů (výstupem tohoto posouzení bude poskytnutí podkladových materiálů a vlastních odborných vyjádření) a realizovat předchozí konzultace s dozorovým úřadem, a to při zohlednění povahy zpracování a informací, jež má Poskytovatel k dispozici;
 - i) v souladu s rozhodnutím Objednatele všechny osobní údaje buď vymaže, nebo vrátí Objednateli, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;
 - j) poskytne Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku Smlouvy, a umožní audity, včetně inspekcí, prováděné Objednatel nebo jiným auditorem, kterého Objednatel pověřil, a k těmto auditům přispěje;
 - k) není oprávněn osobní údaje koncových uživatelů jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy;

- l) umožní Objednateli na vyžádání kontrolu dodržování povinností dle tohoto čl. IX. Smlouvy, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložení seznamu osob s přístupem k osobním údajům či doložení, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby, jak je tato definována níže;
- m) umožní Objednateli přístup do informačního systému užívaného pro zpracování a k probíhajícím operacím zpracování.
8. V souvislosti se zpracováním osobních údajů vede Poskytovatel v souladu s právními předpisy o ochraně osobních údajů záznamy o všech kategoriích činností zpracování prováděných pro Objednatele, jež obsahují zejména:
- a) jméno a kontaktní údaje Poskytovatele, Objednatele a případného zástupce Objednatele nebo Poskytovatele a pověřence pro ochranu osobních údajů;
 - b) kategorie zpracování prováděného pro Objednatele;
 - c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci; a
 - d) popis technických a organizačních bezpečnostních opatření.
- Poskytovatel se na základě písemné výzvy Objednatele zavazuje Objednateli vedené záznamy zpřístupnit.
9. Poskytovatel zajišťuje, kontroluje a odpovídá za:
- a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
 - b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
 - c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
 - d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.
10. Pokud Poskytovatel zjistí, že Objednatel v souvislosti s plněním této Smlouvy porušuje povinnosti podle právních předpisů o ochraně osobních údajů, je povinen jej na to neprodleně upozornit.
11. Vznikne-li Objednateli v důsledku nesplnění povinnosti Poskytovatele dle právních předpisů o ochraně osobních údajů újma (škoda i nemajetková újma), zavazuje se Poskytovatel Objednateli tuto újmu v plném rozsahu nahradit. Újmou vzniklou Objednateli se pro účely tohoto ustanovení rozumí zejména (i) náhrada újmy (škody i nemajetkové újmy) subjektům údajů ve smyslu právních předpisů o ochraně osobních údajů a (ii) pokuty uložené Úřadem pro ochranu osobních údajů či jiným správním úřadem.
12. V případě ukončení této Smlouvy je Poskytovatel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Poskytovatel od Objednatele písemně jiné pokyny, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů.

Zabezpečení osobních údajů

13. Poskytovatel přijal a udržuje taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě,

neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

14. Poskytovatel je povinen zajistit, že přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Poskytovateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním (dále jen „**pověřené osoby**“). Splnění této povinnosti zajistí Poskytovatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou.
15. Poskytovatel dále vhodným způsobem zajistí, že pověřené osoby budou zpracovávat osobní údaje na základě smlouvy s Poskytovatelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Poskytovatelem stanoveném a odpovídajícím této Smlouvě uzavírané mezi Poskytovatelem a Objednatelem a právními předpisy, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.

Poskytovatel přijal a udržuje zejména následující opatření k zajištění úrovně zabezpečení:

 - i. pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;
 - ii. zabránění neoprávněnému přístupu k datovým nosičům;
 - iii. schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;
 - iv. proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
 - v. šifrovaný přenos dat prostřednictvím IT technologií;
 - vi. přístup k osobním údajům mají pouze pověřené osoby Poskytovatele;
 - vii. servery s osobními údaji jsou adekvátně zabezpečeny; a
 - viii. zálohy dat se provádějí do jiné lokality šifrovaným přenosem a přístup k nim mají pouze pověřené osoby Poskytovatele.
16. Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě.
17. Poskytovatel se zavazuje na písemnou žádost Objednatele přijmout v přiměřené lhůtě stanovené Objednatelem další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.
18. V případě zjištění porušení záruk dle odst. 5 tohoto článku IX. Smlouvy je Poskytovatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do 3 pracovních dnů poté, co je k tomu Objednatelem vyzván.
19. V případě, že Poskytovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu, nejpozději do 24 hodin, Objednateli.

X. Ukončení Smlouvy

1. Tato Smlouva může být ukončena vzájemnou dohodou Smluvních stran. Tato dohoda musí být písemná a podepsaná oprávněnými zástupci obou Smluvních stran, jinak je neplatná.
2. Objednatel je oprávněn od této Smlouvy odstoupit v souladu s ustanovením § 2001 a násl. Občanského zákoníku. Odstoupení od této Smlouvy je možné v důsledku, mimo jiné, podstatného porušení Smlouvy Poskytovatelem. Podstatným porušením této Smlouvy je zejména porušení povinností ve smyslu ustanovení § 2002 Občanského zákoníku Poskytovatelem a dále zejména ze strany Poskytovatele opakované nedodání Okruhu řádně nebo včas, předložení Předběžné zprávy k akceptaci v prodlení delším, než 24 (slovy: dvacetčtyři) hodin v případě čl. I. odst. 4 písm. a) této Smlouvy, a než 48 (slovy: čtyřicet osm) hodin v případě čl. I. odst. 4. písm. b) této Smlouvy, porušení povinností dle čl. IX. odst. 6, 7, 8, 9, 12, 14, 15, 16, 17 a 19 této Smlouvy, opakované nebo soustavné porušování povinností, změna poddodavatele nebo člena realizačního týmu v rozporu s postupem dle článku XI. této Smlouvy. Odstoupením od této Smlouvy se závazek zrušuje ke dni doručení odstoupení Poskytovateli.
3. Jednostranné ukončení této Smlouvy nebo skončení trvání Smlouvy z jiného důvodu se nedotýká práva na zaplacení smluvní pokuty nebo úroku z prodlení pokud již dospěl, práva na náhradu újmy vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat Smluvní strany i po odstoupení od této Smlouvy, například ujednání o smluvních pokutách, ujednání o způsobu řešení sporů dle ustanovení § 2005 Občanského zákoníku, článek IX. o ochraně informací, tento odstavec tohoto článku Smlouvy, apod.
4. Objednatel je oprávněn od jakékoliv Dílčí smlouvy odstoupit i bez udání důvodu, a to do dne prokazatelného zahájení předmětu jejího plnění. V případě ukončení Smlouvy zanikají rovněž jednotlivé Dílčí smlouvy, ledaže Objednatel sdělí Poskytovateli, že trvá na splnění konkrétních Dílčích smluv; práva a povinnosti Smluvních stran se při plnění takových Dílčích smluv nadále řídí touto Smlouvou.

XI. Poddodavatelé a členové realizačního týmu

1. Poskytovatel nese plnou odpovědnost za plnění prováděná poddodavatelem se všemi z toho plynoucími důsledky tak, jako by plnil sám.
2. Poskytovatel smí po předchozím souhlasu Objednatele změnit poddodavatele pro provedení části Předmětu plnění dle této Smlouvy. To platí rovněž pro změnu poddodavatele, prostřednictvím kterého Poskytovatel v zadávacím řízení prokazoval kvalifikaci. Takový poddodavatel může být nahrazen pouze poddodavatelem, který se prokáže stejnou nebo vyšší kvalifikací ve vztahu k předmětu příslušné poddodávky, jako poddodavatel původní.
3. Přehled poddodavatelů Poskytovatele, včetně konkrétních částí Předmětu plnění, které bude Poskytovatel prostřednictvím poddodavatelů poskytovat, je uveden v Příloze č. 5 této Smlouvy.
4. Poskytovatel se zavazuje plnit Předmět plnění prostřednictvím členů realizačního týmu uvedených v Příloze č. 6 této Smlouvy. Členové realizačního týmu mohou být měněni pouze po předchozím souhlasu Objednatele. Člen realizačního týmu, který má nahradit původního člena, může být nahrazen pouze osobou se stejnou nebo vyšší kvalifikací ve vztahu k Předmětu plnění, jako původní (nahrazovaný) člen realizačního týmu.

XII. Licence

1. Vzhledem k tomu, že součástí výstupů plnění Poskytovatele dle této Smlouvy je i plnění, které může naplňovat znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o

právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**Autorský zákon**“), je k těmto výstupům plnění Poskytovatele poskytována licence za podmínek sjednaných dále v tomto článku této Smlouvy a to ode dne jejich předání Objednateli.

2. Objednatel je oprávněn veškeré výstupy provádění Předmětu plnění, zejména Závěrečné zprávy, považované za autorské dílo ve smyslu Autorského zákona (dále jen „**Autorská díla**“) užít dle níže uvedených podmínek: Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k Autorskému dílu toto Autorské dílo užít k jakémukoliv účelu, v neomezeném množstevním a územním rozsahu, a to všemi známými způsoby užití a s časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv k takovému Autorskému dílu. Součástí licence je neomezené oprávnění Objednatele provádět jakékoliv modifikace, úpravy, změny Autorského díla a dle svého uvážení do něj zasahovat, zpracovávat ho do dalších Autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob. Objednatel je bez potřeby jakéhokoliv dalšího svolení Poskytovatele oprávněn udělit třetí osobě podlicenci k užití Autorského díla nebo svoje oprávnění k užití Autorského díla třetí osobě postoupit. Licence k Autorskému dílu je poskytována jako výhradní, výlučná a neomezená. Objednatel není povinen licenci využít. Objednatel ode dne nabytí této licence k Autorskému dílu poskytuje Poskytovateli na dobu trvání této Smlouvy licenci k užití Autorského díla v rozsahu nezbytném pro řádné plnění jeho povinností z této Smlouvy.
3. Smluvní strany výslovně prohlašují, že pokud při plnění této Smlouvy vznikne činnost Poskytovatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Poskytovatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů.
4. K veškerým databázím ve smyslu § 88 Autorského zákona (dále jen „**Databáze**“), které vznikly při plnění této Smlouvy a jednotlivých Dílčích smluv, je Objednatel v postavení pořizovatele takové Databáze ve smyslu § 89 Autorského zákona. V ostatních případech Poskytovatel tímto dále Objednateli uděluje právo vytěžovat a zužitkovat veškeré výstupy plnění Předmětu plnění Poskytovatele považované za Databáze za podmínek sjednaných pro poskytnutí licence k Autorským dílům.
5. Odměna za poskytnutí licence k Autorským dílům, vytvoření Databáze a práva vytěžovat a zužitkovat Databáze dle tohoto článku této Smlouvy je zahrnuta v Ceně; bylo-li by z jakéhokoli důvodu třeba určit podrobněji výši odměny za licence a výši odměny za právo vytěžovat a zužitkovat Databáze, a není-li možné výši odměny určit jiným způsobem, pak se Smluvní strany dohodly, že výše odměny tvoří 5 % z Ceny.

XIII. Závěrečná ujednání

1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem zveřejnění v registru smluv dle ZRS (jak je tento pojem definován níže) Objednatel a uzavírá se na dobu určitou, a to do doby vyčerpání maximálního počtu člověkohodin, nejdéle však na dobu 48 měsíců ode dne nabytí účinnosti Smlouvy.
2. V souvislosti s aplikací zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**ZRS**“) se Smluvní strany dohodly na následujícím:
 - a) Smlouva neobsahuje obchodní tajemství žádné ze Smluvních stran a je včetně jejich příloh způsobilá ke zveřejnění v registru smluv ve smyslu ZRS a Smluvní strany se zveřejněním Smlouvy, včetně jejich příloh, souhlasí,

b) Objednatel v souladu s ustanovením § 5 odst. 2 ZRS zašle správci registru smluv elektronický obraz Smlouvy a jejích příloh a metadata vyžadovaná ZRS, Ustanovení se obdobně uplatní na jednotlivé Dílčí smlouvy v ZRS požadovaném rozsahu.

3. Smluvní strany potvrzují, že jsou za ně oprávněni jednat:

Ve věcech smluvních:

za Poskytovatele: [redacted] prokurista společnosti se samostatnou prokurou, tel: [redacted] email: [redacted]

za Objednatele: [redacted] ředitel sekce IKT, [redacted] tel.: [redacted]

Ve věcech věcného plnění:

za Poskytovatele: [redacted] manažer, tel: [redacted] email: [redacted]

za Objednatele: [redacted] vedoucí oddělení bezpečnosti IKT, [redacted] tel.: [redacted]

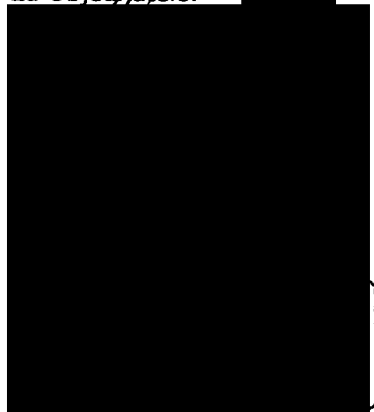
4. Smluvní strany jsou oprávněny změnit výše uvedené oprávněné osoby, jsou však povinny na takovou změnu písemně upozornit druhou Smluvní stranu, a to bez zbytečného odkladu. Taková změna nabývá účinnosti okamžikem, kdy je druhé Smluvní straně doručeno písemné upozornění o změně, přičemž o provedení změny dle tohoto odstavce tohoto článku Smlouvy není nezbytné sepisovat dodatek ke Smlouvě. Všechny dokumenty mající vztah k plnění dle této Smlouvy budou vždy podepsány oprávněnými osobami Smluvních stran nebo jejich pověřenými zástupci, není-li v této Smlouvě stanoveno výslovně jinak.
5. Poskytovatel (včetně případných poddodavatelů) souhlasí s tím, aby subjekty oprávněné dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze Smlouvy s tím, že se Poskytovatel podrobí této kontrole, a bude působit jako osoba povinná ve smyslu ustanovení § 2 písm. e) uvedeného zákona.
6. Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě nebo která mají být učiněna na základě této Smlouvy, musí být učiněna písemně a druhé Smluvní straně doručena buď doporučeným dopisem na adresu uvedenou v záhlaví této Smlouvy, nebo prostřednictvím datové schránky, není-li v této Smlouvě stanoveno nebo mezi Smluvními stranami dohodnuto jinak.
7. Poskytovatel výslovně uvádí, že přebírá nebezpečí změny okolností ve smyslu ustanovení § 1765 odst. 2 a § 2620 odst. 2 (je-li to aplikovatelné) Občanského zákoníku.
8. Smluvní strany se dohodly, že se pro účely této Smlouvy nepoužije ustanovení § 2050 Občanského zákoníku.
9. Poskytovatel se zavazuje, bude-li nezbytná přítomnost zaměstnanců nebo poddodavatelů Poskytovatele v sídle Objednatele, že bude dodržovat závazné platné normy bezpečnosti a ochrany zdraví při práci a vnitřní předpisy Objednatele, se kterými jej Objednatel seznámí, bude se řídit pokyny Objednatele v souvislosti s pohybem osob v rámci budov Objednatele a dále nebude narušovat provoz Objednatele.
10. Případné spory vzniklé z této Smlouvy se Smluvní strany zavazují nejprve vyřešit dohodou. Pokud se Smluvní strany nedohodnou, bude spor řešen před věcně a místně příslušným obecným soudem České republiky dle sídla Objednatele. Rozhodčí řízení je vyloučeno.

11. Ve věcech touto Smlouvou neupravených se tato Smlouva řídí příslušnými ustanoveními Občanského zákoníku. Obchodní zvyklosti nemají přednost před ustanoveními Občanského zákoníku a to ani těmi, které nemají donucující charakter. Na plnění této Smlouvy a Dílčích smluv se nevztahují žádné všeobecné či obdobné obchodní podmínky Poskytovatele. Poskytovatel prohlašuje, že se podrobně seznámil s povinnostmi, které mu vyplývají z této Smlouvy a s důsledky, které způsobí jejich případné nesplnění. V tomto kontextu Smluvní strany výslovně vylučují aplikaci úpravy obsažené v ustanovení § 1799 a § 1800 Občanského zákoníku na tuto Smlouvu a jednotlivé Dílčí smlouvy.
12. Stane-li se některé z ustanovení této Smlouvy zdánlivé, neplatné nebo neúčinné, nebude to mít vliv na platnost a účinnost ustanovení ostatních a na platnost a účinnost této Smlouvy jakožto celku. Zdánlivé, neplatné nebo neúčinné ustanovení bude nahrazeno po vzájemné dohodě Smluvních stran takovým ustanovením, které bude odpovídat svým účinkem co nejbližší původnímu záměru a účelu neplatného či neúčinného ustanovení v ekonomickém i právním smyslu.
13. Tato Smlouva (s výjimkou změny dle čl. XIII. odst. 4 této Smlouvy) může být měněna pouze na základě dohody Smluvních stran, a to ve formě písemně vyhotoveného a vzestupně číslovaného dodatku podepsaného Smluvními stranami. Podpisem Smluvních stran se dodatek stává nedílnou součástí této Smlouvy.
14. Smluvní strany se dohodly na tom, že Poskytovatel není oprávněn činit jednostranná započtení svých pohledávek vzniklých na základě této Smlouvy či v souvislosti s ní vůči jakýmkoli pohledávkám Objednatele.
15. Poskytovatel není bez písemného souhlasu Objednatele oprávněn postoupit práva (včetně pohledávek) ze smluvního vztahu založeného touto Smlouvou na třetí osobu.
16. Tato Smlouva je vyhotovena v 5 (slovy: pěti) stejnopisech, kdy každý z nich má platnost originálu. Z toho 3 (slovy: tři) stejnopisy obdrží Objednatel a 2 (slovy: dva) stejnopisy obdrží Poskytovatel.
17. Součástí této Smlouvy jsou níže uvedené Přílohy:
 - Příloha č. 1 – Specifikace Předmětu plnění
 - Příloha č. 2 - Specifikace ceny Předmětu plnění
 - Příloha č. 3 – Výkaz plnění vzor
 - Příloha č. 4 - Seznam aktuálně platných standardů IKT Objednatele
 - Příloha č. 5 - Přehled poddodavatelů
 - Příloha č. 6 – Realizační tým Poskytovatele
 - Příloha č. 7 - Podrobný popis způsobů uzavírání Dílčích smluv
 - Příloha č. 8 – Vzor Autorizačního dopisu
18. Smluvní strany prohlašují, že si tuto Smlouvu před jejím podpisem přečetly, a že byla uzavřena podle jejich pravé a svobodné vůle. Na důkaz výše uvedeného připojují Smluvní strany své podpisy.



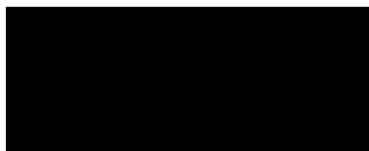
V Praze dne: 24 -07- 2018

Za Objedvatele:



V Praze dne:

Za Poskytovatele:



prokurista se samostatnou prokurou



Specifikace Předmětu plnění

1. Specifikace předmětu plnění

- 1.1. Objednatel, který je správcem informačního systému kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, požaduje (a Poskytovatel je povinen provést) poskytování komplexní služby penetračního testování a bezpečnostní prověrku infrastruktury IIS ČSSZ.
- 1.2. Prováděné penetrační testy musí být Poskytovatelem navrženy jako potenciálně nedestruktivní. Pokud budou některé úkony v prováděných testech potenciálně destruktivní, je Poskytovatel povinen tyto úkony nechat předběžně odsouhlasit Objednatelem a doporučit mu vhodná opatření či jiné kroky pro zamezení vzniku jakékoliv újmy.
- 1.3. Prvotní penetrační test musí mimo využití automatizovaného penetračního testu umožňovat i manuální otestování a ověření kritických zranitelností.
- 1.4. Prvotní penetrační test bude zahrnovat minimálně následujících úkony, které budou popsány v Závěrečné zprávě:
 - seznámení se s IIS ČSSZ a jeho architekturou, získání informací o cílovém systému, jejich identifikace a analýza apod.,
 - zmapování zranitelností – identifikace možných slabín a zranitelností aplikací a prostředí, ve kterém jsou provozovány, dle metodiky u webových aplikací OWASP, případně i podle jiné metodiky, kterou Objednatel, nebo Poskytovatel po dohodě s Objednatelem, používá,
 - využití zranitelností – pokus o získání přístupu pomocí dříve identifikovaných zranitelností s cílem získat uživatelský nebo administrátorský přístup do aplikace nebo operačního systému, neoprávněné získání dat, modifikaci či poškození dat.
- 1.5. Následné penetrační testy se provádějí s cílem potvrdit nebo vyvrátit, že dříve nalezená zranitelnost byla odstraněna.
- 1.6. Následný penetrační test bude prováděn ve stejném rozsahu jako Prvotní penetrační test, pouze s tím rozdílem, že je u Poskytovatele předpokládána znalost testované aplikace z předchozího testování.
- 1.7. Bezpečnostní prověrka infrastruktury prvků IIS ČSSZ se týká následujících částí:
 - aktivních síťových prvků,
 - databází,
 - interních aplikací,
 - provozovaných operačních systémů.
- 1.8. Hlavním cílem bezpečnostní prověrky infrastruktury prvků IIS ČSSZ je posouzení vybraných prvků v kontextu s doporučeními organizací zabývajících se bezpečností informačních technologií (IETF, CVE, CIS apod.).



- 1.9. Poskytovatel identifikuje klíčové prvky v rámci IIS ČSSZ a navrhne doporučení ke zvýšení bezpečnosti.
- 1.10. Bezpečnostní prověrka infrastruktury prvků IIS ČSSZ posoudí stávající infrastrukturu, nebo její část, z pohledu bezpečnosti a doporučí odpovídající nastavení jednotlivých systémů a prvků infrastruktury tak, aby byla v souladu s doporučením výrobců a předních organizací, které se zabývají bezpečností informací.
- 1.11. Součástí Závěrečné zprávy o bezpečnostní prověrce infrastruktury prvků IIS ČSSZ bude hodnocení rizik dle Přílohy 2 Vyhlášky č. 316/2014 Sb.

2. Penetrační testy popis

Poskytovatel předložil závazný vzorový výstup prvotního penetračního testu webové aplikace.
Poskytovatel předložil závazný vzorový postup při provádění penetračních testů.
Poskytovatel předložil závazné vzorové hodnocení rizik prvotních penetračních testů v souladu s Vyhláškou č. 316/2014 Sb.

Vzorový výstup:

Příložené vzorové výstupy vycházejí z reálné realizace penetračních testů a bezpečnostních prověrek v prostředí Zadavatele, přičemž pro potřeby této nabídky resp. rámcové smlouvy byly anonymizovány.

Závěrečná zpráva „Prvotní penetrační test webové aplikace“ je uvedena na dalších listech této rámcové smlouvy.



[Klient]

**Závěrečná zpráva
z externích penetračních testů
[Webová aplikace]
v testovacím prostředí**

Finální report

KPMG Česká republika, s.r.o.

xx. xx. xxxx

Tento report obsahuje 81 stran

Kontrola a schválení dokumentu

Provedené revize

Verze	Autor	Datum	Revize

Tento dokument byl zkontrolován

	Kontrolu provedl/a	Datum kontroly
1		
2		
3		
4		
5		

Tento dokument byl schválen

	Jméno	Podpis	Datum schválení
1			
2			
3			
4			
5			

Obsah

1	Úvod	1
1.1	Rozsah a cíl	1
1.2	Náš přístup	1
1.3	Disclaimer	1
2	Manažerské shrnutí	2
2.1	Detailní soupis zjištění	2
3	Detailní soupis zjištění	5
3.1	Zjištění 1 Po odhlášení je možné se znovu přihlásit bez zadání hesla datové schránky	5
3.1.1	Zjištění	5
3.1.2	Dopad	5
3.1.3	Doporučení	5
3.2	Zjištění 2 MITM útočník může získávat obsah stránek (BREACH)	5
3.2.1	Zjištění	5
3.2.2	Technický dopad	5
3.2.3	Dopad	6
3.2.4	Doporučení	6
3.3	Zjištění 3 Uživatel může potvrdit jinou žádost, než je mu zobrazena	6
3.3.1	Zjištění	6
3.3.2	Technický dopad	6
3.3.3	Dopad	6
3.3.4	Doporučení	7
3.4	Zjištění 4 Server umožňuje šifrování šifrou 3DES	7
3.4.1	Zjištění	7
3.4.2	Dopad	7
3.4.3	Doporučení	7
4	Hodnocení rizik dle ZKB a VKB	8
4.1	Identifikované hrozby a jejich původci	8
4.2	Klasifikace zjištění jako zranitelností	9
4.3	Klasifikace dopadů	9
4.4	Identifikovaná rizika	10
A	Seznam provedených testů	11
B	Postup analýzy rizik	15
B.1	Identifikace hrozeb	15
B.2	Hodnocení zranitelností	15
B.3	Hodnocení dopadů	16
B.4	Stanovení matice hodnocení rizik	18

1 Úvod

Tato zpráva obsahuje souhrn výsledků externích penetračních testů [Webové aplikace] provedených KPMG pro [Klienta] (dále jen „Klient“) v testovacím prostředí.

Externí penetrační testy [Webové aplikace] dle testovací metodiky OWASP Testing Guide v4 byly realizovány jako plnění [Smlouvy] uzavřené na základě [Rámcové smlouvy] dne xx. xx. xxxx (dále rovněž jen „Smlouva“) a v souladu s oboustranně odsouhlasenými podmínkami specifikovanými v Autorizačním dopisu k Provedení penetračních testů [Webové aplikace] dle testovací metodiky OWASP Testing Guide v4 ze dne xx. xx. xxxx.

1.1 Rozsah a cíl

Účelem této bezpečnostní prověrky bylo provedení externího penetračního testu [Webové aplikace]. Testy zahrnovaly testovací prostředí nové verze [Webové aplikace] dostupné na URL <https://xxx.cz> (IP xxx.xxx.xxx.xxx) a související infrastrukturu.

Testy proběhly v první fázi bez znalosti přihlašovacích údajů a ve druhé fázi se znalostí přihlašovacích údajů. Testy dále proběhly bez znalosti prostředí [Webové aplikace] (tzv. black-box testy).

Prostřednictvím penetračních testů jsme simulovali útočníka v roli anonymního uživatele Internetu a útočníka v roli legitimního uživatele služeb [Webové aplikace].

1.2 Náš přístup

Všechny testy byly z počítačové laboratoře v sídle dodavatele – Pobřežní 1a, Praha 186 00.

Testy byly realizovány dle metodik organizace OWASP, zejména dle dokumentů „OWASP Testing Guide“ a „OWASP Testing Guide v4“.

Tato zpráva shrnuje naše zjištění na základě výstupů výše definovaných testů.

1.3 Disclaimer

Bezpečnostní prověrka byla provedena z prostor laboratoře KPMG v Praze v rozmezí od xx.xx. xxxx do xx. xx. xxxx. Naše zjištění jsou tak platná k tomuto datu provedení prověrky.

Jakékoliv změny provedené ve zdrojových kódech webové prezentace a prověřovaných službách na straně serveru mohly mít pozitivní i negativní vliv na úroveň bezpečnosti.

Naše zpráva nesmí být poskytnuta třetí straně bez jasného písemného souhlasu KPMG, kromě vlastníků a kontrolních autorit zadavatele či v důsledku zákonných požadavků.

Vzhledem k omezení přístupu k aplikaci na vybrané IP adresy nebylo možné otestovat, zda je možné se souběžně hlásit z více IP adres.

2 Manažerské shrnutí

V průběhu testování nebyly nalezeny žádné závažné zranitelnosti, které by měly významný vliv na ohrožení bezpečnosti testované aplikace.

V příloze je uvedeno posouzení zjištění z pohledu vyhlášky o kybernetické bezpečnosti; z tohoto pohledu vnímáme všechna příslušná rizika jako nízká.

2.1 Detailní soupis zjištění

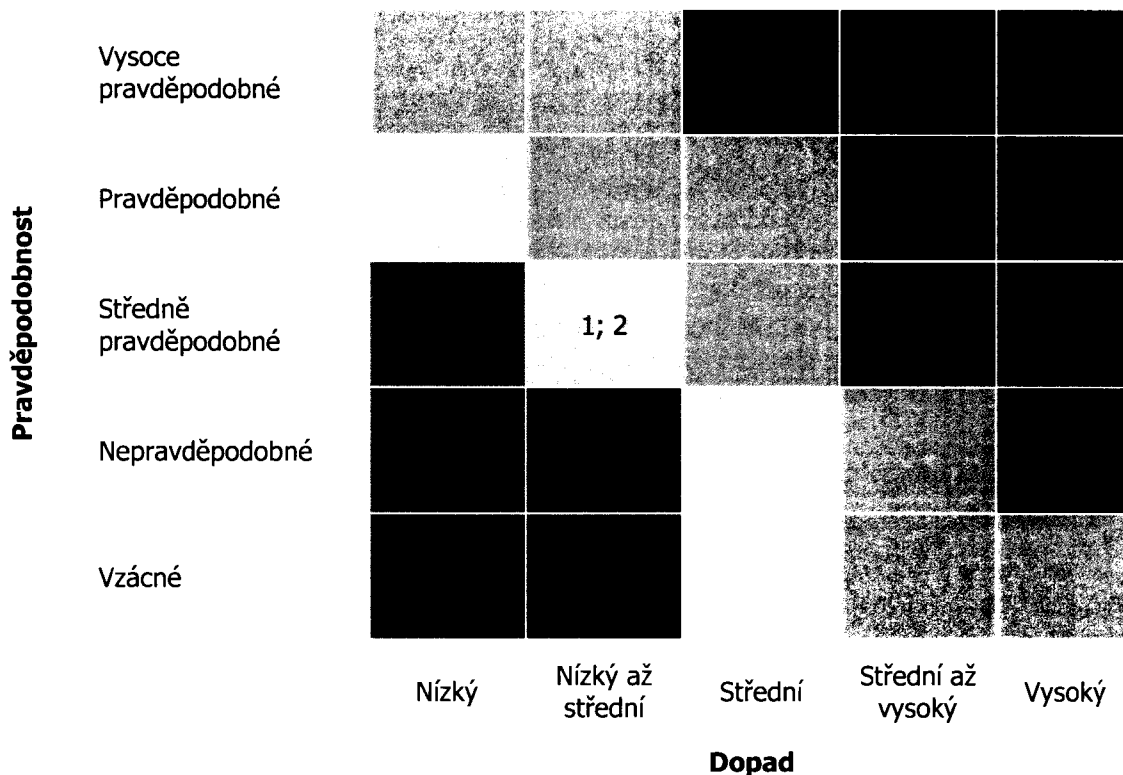
Všechna níže uvedená zjištění se vztahují k verzi [Webové aplikace] implementované v testovacím prostředí a související infrastruktuře, viz rozsah penetračních testů definovaný v kapitole 1.1 *Rozsah a cíl*.

Každé zjištění bylo posouzeno s ohledem na své riziko. Obecně akceptovaná metoda výpočtu potenciálních rizik je použití následujícího vzorce:

$$\text{Riziko} = \text{Pravděpodobnost} \times \text{Dopad}$$

Rizika byla přidána do matice rizik. Matice rizik poskytuje užitečný nástroj pro usnadnění diskusí ohledně zjištění. Položky s vyšším rizikem jsou v matici rizik zobrazeny vpravo nahoře a jsou označeny červeně. Položky s nižším rizikem jsou uvedeny v levé dolní části tabulky a jsou označeny modře. Středně rizikové položky představují odstíny žluté a oranžové barvy uprostřed tabulky.

Následující obrázek je grafickým znázorněním matice rizik. Čísla v buňkách shrnují všechna zjištění detailně popsaná v tomto reportu a jsou kategorizovaná v souladu s uvedeným rizikovým hodnocením.



Obrázek 1 – Klasifikace rizik v matici rizik

Tímto způsobem je zobrazeno vzestupné hodnocení rizika na čtyřech úrovních (modrá, žlutá, oranžová a červená). Níže uvedená tabulka blíže popisuje jednotlivé úrovně.

Barva	Úroveň rizika	Popis
Červená	První úroveň zájmu managementu	Zjištění v této oblasti jsou vysoce kritická a je požadováno okamžité nápravné opatření.
	Druhá úroveň zájmu managementu	Zjištění v této oblasti jsou závažná a je nutné naplánovat nápravná opatření.
Žlutá	Rozhodnutí managementu	Zjištění v této oblasti jsou na takové úrovni, kdy by měla být nápravná opatření naplánována.
	Nízké riziko	U těchto zjištění je vyžadována pozornost, ale opatření nemusí být konkrétně určena, dokud se nevyřeší problémy s vyšším rizikem.

Tabulka 1 – Kategorie rizik v matici rizik

Níže uvedená tabulka obsahuje seznam zjištění spolu s jejich kategorií v matici rizik. Popisy zjištění, souvisejících rizik a doporučení pro zlepšení jsou detailně popsány v další kapitole.

Zařazení matice rizik	ID zjištění	Zjištění	Pravděpodobnost	Dopad
Žlutá	1	Po odhlášení je možné se znovu přihlásit bez zadání hesla datové schránky	Středně Pravděpodobné	Nízký až střední
Žlutá	2	MITM útočník může získávat obsah stránek (BREACH)	Středně pravděpodobné	Nízký až střední
	3	Uživatel může potvrdit jinou žádost, než je mu zobrazena	Nepravděpodobné	Nízký
	4	Server umožňuje šifrování šifrou 3DES	Vzácné	Nízký až střední

Tabulka 2 – Seznam zjištění vztahujících se k [Webové aplikaci]

3 Detailní soupis zjištění

Všechna níže uvedená zjištění se vztahují k verzi [Webové aplikace] implementované v testovacím prostředí a související infrastruktuře, viz rozsah penetračních testů definovaný v kapitole 1.1 *Rozsah a cíl*.

3.1 Zjištění 1 Po odhlášení je možné se znovu přihlásit bez zadání hesla datové schránky

3.1.1 Zjištění

V některých případech došlo k tomu, že uživatel byl odhlášen (podle zobrazeného textu). Pokud se pokusil přihlásit, byl přihlášen bez provedení přesměrování na přihlašovací stránku datových schránek.

K této situaci například dojde, když uživatel zavře okno portálu, počká cca 10 minut, a znovu otevře stránku portálu.

Při odhlášení tlačítkem odhlásit tato atypická situace nevzniká.

Po uplynutí výrazně delší doby od odhlášení je uživatel plně odhlášen a k popsané situaci nedochází.

3.1.2 Dopad

Uživatel může přenechat „odhlášený“ počítač útočnickovi, který se takto dokáže znovu přihlásit do účtu uživatele. Poté může přímo získávat nebo rozesílat soukromé údaje uživatele. Nenalezli jsme způsob, jak v aplikaci přístup využít k vyvolání akce závažnější než únik dat.

K využití zranitelnosti může dojít buď náhodou, kdy následující uživatel počítače otevře v relativně úzkém časovém okně stejnou aplikaci, nebo při záměrném „vedení“ uživatele útočnickem. V prvním případě může následný uživatel otevřít novou aplikaci stejně dobře dříve než po deseti minutách a je přihlášen okamžitě (se stejným dopadem), druhý případ nevnímáme jako zcela reálný.

3.1.3 Doporučení

Doporučujeme v případě odhlášení zajistit, že veškeré autorizační informace jsou zneplatněny.

3.2 Zjištění 2 MITM útočník může získávat obsah stránek (BREACH)

3.2.1 Zjištění

Řada stránek vloží do své odpovědi celé požadované URL (např. v link tagu, `liferay.currentURL` a dalších javascriptových proměnných). Klient si může vyžádat komprimaci odpovědi serveru metodou `gzip` nebo `deflate`.

3.2.2 Technický dopad

Pokud má útočník přístup k zašifrované komunikaci mezi serverem a klientem – tedy může pozorovat délku přenášených dat, a pokud zároveň může klienta přimět k vykonávání řady dotazů, může zjistit obsah vrácené stránky nebo její citlivé části pozorováním délky odpovědi při

různém vloženém textu (pokud je vložený text prodlužován tak, že stále odpovídá již existujícímu textu ve stránce, délka zkomprimovaného textu se nemění, v opačném případě ano).

Tato slabina je označována jako BREACH. Takto získat pouze obsah stránky, nikoliv její hlavičky (tedy nelze získat například obsah session-id cookie).

3.2.3 Dopad

Nebyli jsme schopni v textu stránek nalézt údaje umožňující přihlášení nebo převzetí sezení.

Mezi údaje, které je možné získat, patří například informace o uživateli nebo o poslaných žádostech.

3.2.4 Doporučení

Možné reakce jsou:

- akceptovat riziko s tím, že v textu HTTP odpovědi nesmí být v budoucnu citlivé údaje,
- omezit riziko monitoringem útoku na straně IDS/monitoringu,
- zakázat komprimaci HTTP stránek (může vést k nárůstu provozu),
- zakázat komprimaci stránky při absenci správné hlavičky Referer,
- zakázat komprimaci stránky, pokud obsahuje citlivé údaje.

3.3 Zjištění 3 Uživatel může potvrdit jinou žádost, než je mu zobrazena

3.3.1 Zjištění

Uživateli je před finálním odesláním žádosti předložen její text k potvrzení. Pokud v mezidobí je ve stejném sezení vytvořena další žádost, odesláním potvrzení potvrdí novější žádost.

To indikuje, že potvrzení žádosti neobsahuje identifikaci potvrzovaného obsahu.

3.3.2 Technický dopad

Pokud se útočníkovi podaří přimět uživatele k vytvoření další žádosti (metodou CSRF, vložení linku a podobně) v době mezi vytvořením a podáním žádosti, může přimět uživatele k potvrzení falešné žádosti.

Kromě toho vzhledem k tomu, že potvrzení neobsahuje informaci specifickou pro danou žádost (autorizační token), lze očekávat, že útočník může metodou CSRF poslat žádost i její potvrzení.

Vzhledem k omezenému časovému oknu pro testování jsme nerealizovali útok do úplného konce.

3.3.3 Dopad

Útočník může vygenerovat na účet uživatele žádost dle vlastní volby. To může vést k úniku dat oprávněného uživatele.

- 3.3.4 Doporučení**
Doporučujeme pro každou žádost vygenerovat unikátní autorizační token, vložit jej do formuláře pro potvrzení, a kontrolovat jeho správnost při zpracování potvrzení.

3.4 Zjištění 4 Server umožňuje šifrování šifrou 3DES

- 3.4.1 Zjištění**
Server umožňuje šifrování šifrou 3DES.
Server nepovolí přenést více než 100 stránek na jedno spojení.
- 3.4.2 Dopad**
Tato šifra již není považována za bezpečnou, pokud se přenáší více než cca 32GB s jedním klíčem. Vzhledem k omezení na počet přenesených stránek na jedno spojení by bylo nutné přenést cca 320MB v každé stránce; přestože toto nemůžeme vyloučit (i vzhledem k možnosti útočníka vkládat text do stránky), nepovažujeme to za pravděpodobné.
- 3.4.3 Doporučení**
Doporučujeme monitorovat abnormálně objemné dotazy a odpovědi ze serveru.

4 Hodnocení rizik dle ZKB a VKB

Tato kapitola obsahuje hodnocení rizik souvisejících se zjištěními uvedenými v tomto dokumentu dle požadavků vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti (VKB), a dle kritérií stanovených v této vyhlášce.

4.1 Identifikované hrozby a jejich původci

Jako relevantní byly zvažovány následující hrozby a jejich původci.

	Hrozba	Původce	Hodnocení
1.	Kybernetický útok na systém s úmyslem získání osobních dat z prostředí infrastruktury. Vzhledem k počtu potenciálních útočníků s takovýmto přístupem a relativně nízké využitelnosti dat tohoto typu oproti jiným datům, která takovouto sítí prochází, klasifikujeme pravděpodobnost hrozby jako nízkou.	Útočník s přístupem na infrastrukturu přenosu (např. zaměstnanec úřadu nebo společnosti, která zajišťuje infrastrukturu pro přístup k aplikacím)	Nízká
2.	Kybernetický útok na systém s úmyslem získání osobních nebo jinak citlivých dat. Hrozbu hodnotíme jako střední, protože útočník musí mít základní povědomí o existenci systému, musí mít zájem na datech v systému, a tento způsob získání dat je pro něj jednodušší než alternativní možnosti.	Externí útočník, který má zájem a prostředky uskutečnit svoje hrozby	Střední
3.	Oportunistický útok na zjevnou chybu systému. Vzhledem k dostupnosti aplikace pro velké množství uživatelů hodnotíme hrozbu jako střední.	Útočník s možností a vůlí využít náhodně získaný přístup k údajům	Střední

4.2 Klasifikace zjištění jako zranitelností

Zranitelnosti zjištěné během testu jsme v souladu s metodologií klasifikovali takto.

Zjištění	Hodnocení
Po odhlášení je možné se znovu přihlásit bez zadání parametrů schránky	Vysoká
MITM útočník může získávat obsah stránek (BREACH)	Střední
Uživatel může potvrdit jinou žádost než je mu zobrazena	Nízká
Server umožňuje šifrování šifrou 3DES	Nízká

4.3 Klasifikace dopadů

Možné dopady byly klasifikovány takto:

Popis	Dopad
Finanční pokuta za nedodržení ochrany osobních údajů za malý rozsah úniku dat (do 5 mil. CZK).	Nízký
Náhrada škod jednotkám klientů postižených únikem osobních dat. Předpokládáme, že výše vzniklé prokazatelné škody nebude více než 5 mil.	Nízký
Zahlcení následných systémů velkým množstvím požadavků.	Nízký

4.4 Identifikovaná rizika

Z pohledu ZKB vnímáme všechna zvažovaná rizika využívající zjištěných slabín jako nízká.

Zranitelnost/Popis rizika	Velikost hrozby	Závažnost zranitelnosti	Úroveň dopadu	Hodnota rizika
Po odhlášení je možné se znovu přihlásit bez zadání parametrů schránky Oportunistický útočník s fyzickým přístupem k zařízení, na kterém byl přihlášen oprávněný uživatel, získá přístup k sezení uživatele, který ověřil, že je odhlášen.	Střední	Vysoká	Nízký	
MITM útočník může získávat obsah stránek (BREACH) Útočník s přístupem na infrastrukturu přenosu úspěšně uskuteční BREACH útok. Tím získá citlivé osobní údaje ze stránky.	Nízká	Střední	Nízký	
Server umožňuje šifrování šifrou 3DES Útočník s přístupem na infrastrukturu přenosu získá potřebný rozsah dat k uskutečnění SWEET32 útoku na uživatele. Tím získá přístup k jeho sezení a toho využije k získání osobních dat uživatele dostupných přes aplikaci, nebo k zahlcení systémů množstvím zbytečných žádostí.	Nízká	Nízká	Nízký	
Uživatel může potvrdit jinou žádost než je mu zobrazena Externí útočník se zájmem na získání osobních dat přiměje uživatele k návštěvě stránky, která nechá vygenerovat dotaz generující a následně potvrzující žádost, ve které zašle citlivé údaje na útočníkem definovanou adresu.	Střední	Nízká	Nízký	

A Seznam provedených testů

ID testu	Popis	Realizace testu
OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	N/A – neveřejná adresa
OTG-INFO-002	Fingerprint Web Server	Testováno
OTG-INFO-003	Review Webserver Metafiles for Information Leakage	Testováno
OTG-INFO-004	Enumerate Applications on Webserver	Testováno
OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage	Testováno
OTG-INFO-006	Identify application entry points	Testováno
OTG-INFO-007	Map execution paths through application	Testováno
OTG-INFO-008	Fingerprint Web Application Framework	Testováno
OTG-INFO-009	Fingerprint Web Application	Testováno
OTG-INFO-010	Map Application Architecture	Testováno
OTG-CONFIG-001	Test Network/Infrastructure Configuration	Testováno
OTG-CONFIG-002	Test Application Platform Configuration	Testováno
OTG-CONFIG-003	Test File Extensions Handling for Sensitive Information	Testováno
OTG-CONFIG-004	Review Old, Backup and Unreferenced Files for Sensitive Information	Testováno
OTG-CONFIG-005	Enumerate Infrastructure and Application Admin Interfaces	Testováno
OTG-CONFIG-006	Test HTTP Methods	Testováno
OTG-CONFIG-007	Test HTTP Strict Transport Security	Testováno
OTG-CONFIG-008	Test RIA cross domain policy	Testováno
OTG-IDENT-001	Test Role Definitions	N/A
OTG-IDENT-002	Test User Registration Process	N/A
OTG-IDENT-003	Test Account Provisioning Process	N/A
OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account	N/A
OTG-IDENT-005	Testing for Weak or unenforced username policy	N/A
OTG-AUTHN-001	Testing for Credentials Transported over an Encrypted Channel	N/A
OTG-AUTHN-002	Testing for default credentials	N/A

OTG-AUTHN-003	Testing for Weak lock out mechanism	N/A
OTG-AUTHN-004	Testing for bypassing authentication schema	N/A
OTG-AUTHN-005	Test remember password functionality	N/A
OTG-AUTHN-006	Testing for Browser cache weakness	Testováno
OTG-AUTHN-007	Testing for Weak password policy	Testováno částečně (změna hesla povolena, nelze provést bez znalosti starého hesla)
OTG-AUTHN-008	Testing for Weak security question/answer	N/A
OTG-AUTHN-009	Testing for weak password change or reset functionalities	N/A
OTG-AUTHN-010	Testing for Weaker authentication in alternative channel	N/A
OTG-AUTHZ-001	Testing Directory traversal/file include	Testováno
OTG-AUTHZ-002	Testing for bypassing authorization schema	N/A
OTG-AUTHZ-003	Testing for Privilege Escalation	N/A
OTG-AUTHZ-004	Testing for Insecure Direct Object References	Testováno
OTG-SESS-001	Testing for Bypassing Session Management Schema	N/A
OTG-SESS-002	Testing for Cookies attributes	Testováno
OTG-SESS-003	Testing for Session Fixation	Testováno
OTG-SESS-004	Testing for Exposed Session Variables	N/A
OTG-SESS-005	Testing for Cross Site Request Forgery (CSRF)	Testováno
OTG-SESS-006	Testing for logout functionality	Testováno
OTG-SESS-007	Test Session Timeout	Testováno
OTG-SESS-008	Testing for Session puzzling	Testováno
OTG-INPVAL-001	Testing for Reflected Cross Site Scripting	Testováno
OTG-INPVAL-002	Testing for Stored Cross Site Scripting	Testováno
OTG-INPVAL-003	Testing for HTTP Verb Tampering	Testováno
OTG-INPVAL-004	Testing for HTTP Parameter pollution	Testováno
OTG-INPVAL-005	Testing for SQL Injection	Testováno
OTG-INPVAL-006	Testing for LDAP Injection	Testováno
OTG-INPVAL-007	Testing for ORM Injection	Testováno
OTG-INPVAL-008	Testing for XML Injection	Testováno

OTG-INPVAL-009	Testing for SSI Injection	Testováno
OTG-INPVAL-010	Testing for XPath Injection	Testováno
OTG-INPVAL-011	IMAP/SMTP Injection	N/A
OTG-INPVAL-012	Testing for Code Injection	Testováno
OTG-INPVAL-013	Testing for Command Injection	Testováno
OTG-INPVAL-014	Testing for Buffer overflow	Testováno
OTG-INPVAL-015	Testing for incubated vulnerabilities	Testováno
OTG-INPVAL-016	Testing for HTTP Splitting/Smuggling	Testováno
OTG-ERR-001	Analysis of Error Codes	Testováno
OTG-ERR-002	Analysis of Stack Traces	Testováno
OTG-CRYPST-001	Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection	Testováno
OTG-CRYPST-002	Testing for Padding Oracle	Netestováno
OTG-CRYPST-003	Testing for Sensitive information sent via unencrypted channels	Testováno
OTG-BUSLOGIC-001	Test Business Logic Data Validation	Testováno
OTG-BUSLOGIC-002	Test Ability to Forge Requests	Testováno
OTG-BUSLOGIC-003	Test Integrity Checks	Testováno
OTG-BUSLOGIC-004	Test for Process Timing	Netestováno
OTG-BUSLOGIC-005	Test Number of Times a Function Can be Used Limits	Testováno
OTG-BUSLOGIC-006	Testing for the Circumvention of Work Flows	Testováno
OTG-BUSLOGIC-007	Test Defenses Against Application Mis-use	Testováno
OTG-BUSLOGIC-008	Test Upload of Unexpected File Types	N/A
OTG-BUSLOGIC-009	Test Upload of Malicious Files	N/A
OTG-CLIENT-001	Testing for DOM based Cross Site Scripting	Testováno
OTG-CLIENT-002	Testing for JavaScript Execution	Testováno
OTG-CLIENT-003	Testing for HTML Injection	Testováno
OTG-CLIENT-004	Testing for Client Side URL Redirect	Testováno

OTG-CLIENT-005	Testing for CSS Injection	Testováno
OTG-CLIENT-006	Testing for Client Side Resource Manipulation	Testováno
OTG-CLIENT-007	Test Cross Origin Resource Sharing	Testováno
OTG-CLIENT-008	Testing for Cross Site Flashing	N/A
OTG-CLIENT-009	Testing for Clickjacking	Testováno
OTG-CLIENT-010	Testing WebSockets	N/A
OTG-CLIENT-011	Test Web Messaging	N/A
OTG-CLIENT-012	Test Local Storage	N/A

B Postup analýzy rizik

V této sekci popisujeme obecný postup použitý v analýze rizik uvedené v kapitole 4 *Hodnocení rizik dle ZKB a VKB*.

B.1 Identifikace hrozeb

V analýze rizik byly v souladu s § 4 odstavcem (4) Vyhlášky zvažovány následující hrozby:

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity fyzické osoby,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. kybernetický útok z komunikační sítě,
6. škodlivý kód (například viry, spyware, trojské koně),
7. nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,
8. narušení fyzické bezpečnosti,
9. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
10. zneužití nebo neoprávněná modifikace údajů,
11. trvale působící hrozby,
12. odcizení nebo poškození aktiva.

Hrozby byly v rámci analýzy rizik hodnoceny podle kritérií uvedených v příloze č. 2 k Vyhlášce.

Pro hodnocení hrozeb byla použita následující stupnice:

Koeficient	Úroveň	Popis
10%	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
30%	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
200%	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
1200%	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

B.2 Hodnocení zranitelností

Zranitelnosti byly v rámci analýzy rizik hodnoceny podle kritérií uvedených v příloze č. 2 k Vyhlášce. Pro jejich klasifikaci byla použita stupnice dle vyhlášky:

Stupnice pro hodnocení zranitelnosti

Koeficient	Úroveň	Popis
0	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, která jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
0,5	Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
0,7	Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
1,0	Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

B.3 Hodnocení dopadů

Pro hodnocení dopadů byla použita následující matice založená na příloze č. 2 k Vyhlášce.

Matrice pro hodnocení dopadů

Oblast	Nízký (1)	Střední (10)	Vysoký (100)	Kritický (1000)
Dopad na hospodaření [Klienta]	Finanční nebo materiální ztráty do 5 000 000 Kč	Finanční nebo materiální ztráty od 5 000 000 Kč do 50 000 000 Kč	Finanční nebo materiální ztráty od 50 000 000 Kč do 500 000 000 Kč	Finanční nebo materiální ztráty převyšující 500 000 000 Kč
Dopad na veřejnost	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2 500 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2 501 do 25 000 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25 000 osob
Finanční dopad na vedení [Klienta]	Finanční postih člena vedení ve výši do 50 tis. Kč	Finanční postih člena vedení ve výši od 50 do 200 tis. Kč	Finanční postih člena vedení vyšší než 200 tis. Kč	
Personální dopady na vedení [Klienta]	Disciplinární řízení	Odvolení z funkce, vedení trestního řízení	Zákaz výkonu povolání, trest odnětí svobody až do 3 let	Odvolení celého vedení [Klienta]
Nefinanční dopady	Negativní publicita v médiích s dosahem do 100 tis. obyvatel trvající méně než 1 týden	Negativní publicita v médiích s dosahem do 100 tis. obyvatel trvající více jak 1 týden	Negativní celostátní publicita trvající 1 měsíc	
	Negativní celostátní publicita trvající 1 den	Negativní celostátní publicita trvající do 1 týdne	Otevření diskuse o zrušení či výrazném omezení funkce [Klienta]	Zrušení či výrazné omezení funkce [Klienta]

B.4 Stanovení matice hodnocení rizik

Dopady byly v rámci analýzy rizik oceňovány podle kritérií uvedených v příloze č. 2 k vyhlášce 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Vzhledem k tomu, že jsme neměli k dispozici platnou metodiku [Klienta] pro analýzu a hodnocení rizik jsme na základě běžně používané praxe definovali metodiku takto:

Pro ocenění rizik byly stanoveny následující 4 úrovně rizik.

Název úrovně rizika		Naléhavost a intenzita reakce	Hodnota výše rizika	Barevné označení
1.	Malé riziko	Je nutné pouze registrovat a sledovat, zda se nezvyšuje	0-1	
2.	Střední riziko	Vyžaduje soustavnou pozornost a postupné zavádění opatření na jejich eliminaci	1-10	
3.	Velmi vysoké riziko	Vyžaduje okamžité zahájení plánování opatření na eliminaci rizika a alokaci potřebných zdrojů.	10-100	
4.	Kritické riziko	Vyžaduje neodkladné řešení, zapojení všech disponibilních zdrojů a zapojení nevyššího vedení	100+	

Rizika jsou klasifikována na základě síly hrozby, stupně zranitelnosti a velikosti dopadu jako $\min(100, h \times z) / 100 \times d$, tedy takto:

- je odhadnuta roční pravděpodobnost využití příslušné hrozby daným aktivem vynásobením pravděpodobnosti hrozby (viz stupnici hrozeb) a koeficientem závažnosti slabiny (viz stupnici slabin),
- výsledek je omezen na maximálně 100%,
- tato pravděpodobnost vynásobená koeficientem velikosti dopadu určuje hodnotu rizika, podle které je zařazeno do úrovně.

Pro názornost uvádíme mapování získané pravděpodobnosti a dopadu na velikost rizika graficky; v posledním sloupci je uvedeno, jakou maximální pravděpodobnost může dosáhnout hrozba o dané síle (při kritické zranitelnosti).

Dopad	Nízký	Střední	Vysoký	Kritický	Maximum pro hrozby (kritická zranitelnost)
Pravděpodobnost					
pod 0.1%					
0.1% až 1%				Střední	
1% až 10%			Střední		Nízká
10% až 100%		Střední		Kritické	Střední
100%	Střední		Kritické	Kritické	Vysoká, Kritická



3. Bezpečnostní prověrka prvků IIS ČSSZ popis

Poskytovatel předložil závazný vzorový výstup bezpečnostní prověrky infrastruktury.
Poskytovatel předložil závazné vzorové hodnocení rizik bezpečnostní prověrky infrastruktury v souladu s Vyhláškou č. 316/2014 Sb.

Vzorový výstup:

Přiložené vzorové výstupy vycházejí z reálné realizace penetračních testů a bezpečnostních prověrek v prostředí Zadavatele, přičemž pro potřeby této nabídky resp. rámcové smlouvy byly anonymizovány.

Závěrečná zpráva „Bezpečnost prověrky infrastruktury“ je uvedena na dalších listech této rámcové smlouvy.

[Klient]

**Bezpečnostní prověrka
[Infrastruktury]**

Závěrečná zpráva

KPMG Česká republika, s.r.o.

xx. xx. xxxx

Tento report obsahuje 81 stran

Kontrola a schválení dokumentu

Provedené revize

Verze	Autor	Datum	Revize

Tento dokument byl zkontrolován

	Kontrolu provedl/a	Datum kontroly
6		
7		
8		
9		
10		

Tento dokument byl schválen

	Jméno	Podpis	Datum schválení
6			
7			
8			
9			
10			

Obsah

1	Úvod	1
1.1	Použité metody	1
1.2	Odchytky oproti autorizačnímu dopisu	1
1.3	Struktura dokumentu	1
2	Manažerské shrnutí	3
2.1	Detailní soupis zjištění	3
3	Soupis zjištění	6
3.1	Zjištění 1 Parametry hesel	6
3.1.1	Zjištění	6
3.1.2	Dopad	6
3.1.3	Doporučení	6
3.2	Zjištění 2 Řízení práv uživatelů	6
3.2.1	Zjištění	6
3.2.2	Dopad	7
3.2.3	Doporučení	7
3.3	Zjištění 3 Vypnutý firewall	7
3.3.1	Zjištění	7
3.3.2	Dopad	7
3.3.3	Doporučení	7
3.4	Zjištění 4 Defaultní konfigurace většiny bezpečnostních nastavení	7
3.4.1	Zjištění	7
3.4.2	Dopad	8
3.4.3	Doporučení	8
4	Hodnocení rizik dle ZKB a VKB	9
4.1	Identifikované hrozby a jejich původci	9
4.2	Klasifikace zjištění jako zranitelností	10
4.3	Klasifikace dopadů	10
4.4	Identifikovaná rizika	10
A	Identifikované odchytky od požadavků standardu CIS	12
A.1	Windows 2008 R2	12
A.2	Oracle Linux	13
A.3	Oracle databáze	14
A.4	Webové servery Apache	14
A.5	Apache Tomcat	15
B	Postup analýzy rizik	16
B.1	Identifikace hrozeb	16
B.2	Hodnocení zranitelností	17

B.3	Hodnocení dopadů	17
B.4	Stanovení matice hodnocení rizik	19
C	Výstupy skriptů CIS-CAT a detailní seznam systémů	22

1 Úvod

Tento dokument shrnuje výsledky Bezpečnostní prověrky [Infrastruktury] (dále jen „prověrka“ nebo „bezpečnostní prověrka“) provedené společností KPMG Česká republika, s.r.o. (dále jen „KPMG“) pro [Klienta] (dále jen „Klient“).

Prověrka byla realizována jako plnění [Smlouvy] uzavřené na základě [Rámcové smlouvy] dne xx. xx. xxxx (dále rovněž jen „Smlouva“), v návaznosti na odsouhlasený „Rámcový plán“ ze dne xx. xx. xxx a v souladu s oboustranně odsouhlasenými podmínkami specifikovanými v Autorizačním dopisu z xx. xx. xxxx.

1.1 Použité metody

Prezentované výsledky vyplývají ze zjištěných hodnot konfiguračních parametrů, které byly získány na základě spouštění auditních skriptů a na základě předaných konfiguračních souborů. Zjištěné hodnoty byly porovnány s doporučenými cílovými hodnotami. Na základě zjištěných nastavení a jejich odchylek od doporučení byla formulována zjištění tam, kde vnímáme negativní dopad na bezpečnost. Plný seznam identifikovaných odchylek je uveden v příloze.

1.2 Odchyly oproti autorizačnímu dopisu

Z objektivních důvodů byly po dohodě s pracovníky [Klienta] v rámci postupu bezpečnostní prověrky provedeny následující odchyly oproti autorizačnímu dopisu a schválenému plánu v těchto oblastech:

- nebyly předány výsledky skriptů z prostředí MS SQL,
- skripty byly spouštěny na testovacích serverech pracovníky dodavatele bez asistence auditora,
- rozsah systémů byl mírně modifikován oproti původním očekáváním (různé verze Windows serverů, atp.).

1.3 Struktura dokumentu

V dokumentu je uvedeno souhrnné vyhodnocení výsledků bezpečnostní prověrky pro zkoumané servery, poté jsou uvedeny detaily jednotlivých zjištění.

Každé zjištění obsahuje:

- název/stručný popis zjištění,
- popis dopadu zjištění v kontextu [Klienta],
- doporučení na odstranění zjištění.

Dále je v příloze A přehled hodnocení zjištěných odchylek od požadavků CIS Level 1, případně vlastní seznam odchylek, pokud není součástí výstupu automatického skriptu v příloze C. Seznam je členěn podle typů serverů a obsahuje:

- ení je možné se znovu phodnocení odchylky.
- hodnocení odchylky.

Doporučené hodnoty konfiguračních parametrů byly stanoveny na základě

- CIS-CAT skriptů platných v dané době pro

- Windows Server 2008,
- Oracle Linux 6,
- Oracle databázový server 12c,
- CIS benchmarků pro
 - Apache http server 2.4 verze 1.3.1 z 17. 8. 2017,
 - Apache Tomcat 8 verze 1.0.1 z 16. 9. 2016.

2 Manažerské shrnutí

Výsledky porovnání nastavení konfigurací Windows serverů, Oracle Linux serverů a databázového serveru s požadavky standardu CIS ukazují, že řada – ne-li většina – relevantních nastavení byla ponechána v defaultním stavu. To má za následek relativně nižší odolnost serverů oproti hrozbám útoku zejména z vnitřní sítě. Oproti obdobnému zjištění pro stanice Windows¹ je riziko omezeno existujícími opatřeními jako například segmentace sítě, avšak na druhou stranu možný dopad je zvýšen významností serverů.

Jako příklady chybějících zabezpečení proti útokům z vnitřní sítě můžeme uvést:

- Vypnuté firewally ve vnitřní síti.
- Chybějící nastavení chránicí proti pass-the-hash a podobným útokům a Nevynucování podepisování komunikace v rámci domény.
- Nedodržování principu minimálních oprávnění.
- Nepoužívání pokročilých nástrojů pro zabezpečení zejména Linuxových systémů, jako je kontrola integrity (aide).
- Nevynucování požadavků na hesla pro lokální účty v systémech (doménové kontrolery a doménové účty nebyly předmětem testu). To zakládá i riziko z pohledu požadavků souladu se zákonnými předpisy.

Žádné ze zjištění nepovažujeme za bezprostředně ohrožující bezpečnost společnosti.

Konfigurace Apache web serverů a Apache Tomcat serverů byly až na drobné odchylky v souladu s relevantními požadavky CIS úrovně 1, v řadě případů byly implementovány i požadavky CIS úrovně 2.

2.1 Detailní soupis zjištění

Všechna níže uvedená zjištění se vztahují k testovaným serverům.

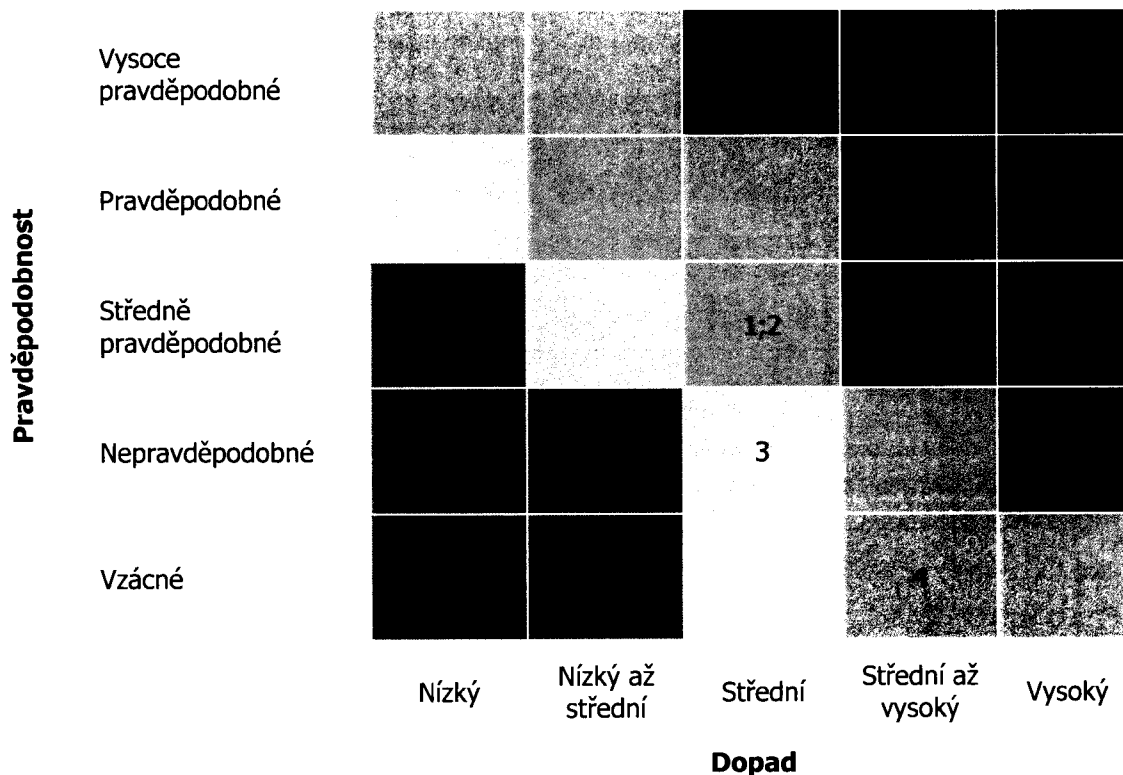
Každé zjištění bylo posouzeno s ohledem na své riziko. Obecně akceptovaná metoda výpočtu potenciálních rizik je použití následujícího vzorce:

$$\text{Riziko} = \text{Pravděpodobnost} \times \text{Dopad}$$

Rizika byla přidána do matice rizik. Matice rizik poskytuje užitečný nástroj pro usnadnění diskusí ohledně zjištění. Položky s vyšším rizikem jsou v matici rizik zobrazeny vpravo nahoře a jsou označeny červeně. Položky s nižším rizikem jsou uvedeny v levé dolní části tabulky a jsou označeny modře. Středně rizikové položky představují odstíny žluté a oranžové barvy uprostřed tabulky.

Následující obrázek je grafickým znázorněním matice rizik. Čísla v buňkách shrnují všechna zjištění detailně popsána v tomto reportu a jsou kategorizována v souladu s uvedeným rizikovým hodnocením.

¹ viz Závěrečná zpráva z bezpečnostní prověrky konfigurací stanice a notebooků Windows 7 verze x.x z xx. xx. xxxx.



Obrázek 2 – Klasifikace rizik v matici rizik

Tímto způsobem je zobrazeno vzestupné hodnocení rizika na čtyřech úrovních (modrá, žlutá, oranžová a červená). Níže uvedená tabulka blíže popisuje jednotlivé úrovně.

Barva	Úroveň rizika	Popis
	První úroveň zájmu managementu	Zjištění v této oblasti jsou vysoce kritická a je požadováno okamžité nápravné opatření.
	Druhá úroveň zájmu managementu	Zjištění v této oblasti jsou závažná a je nutné naplánovat nápravná opatření.
Žlutá	Rozhodnutí managementu	Zjištění v této oblasti jsou na takové úrovni, kdy by měla být nápravná opatření naplánována.
	Nízké riziko	U těchto zjištění je vyžadována pozornost, ale opatření nemusí být konkrétně určena, dokud se nevyřeší problémy s vyšším rizikem.

Tabulka 1 – Kategorie rizik v matici rizik

Níže uvedená tabulka obsahuje seznam zjištění spolu s jejich kategorií v matici rizik. Popisy zjištění, souvisejících rizik a doporučení pro zlepšení jsou detailně popsány v další kapitole.

Zařazení matice rizik	ID zjištění	Zjištění	Pravděpodobnost	Dopad
Červená	1	Parametry hesel	Středně pravděpodobné	Střední
Červená	2	Řízení práv uživatelů	Středně pravděpodobné	Střední
Červená	4	Defaultní konfigurace	Vzácné	Střední až vysoký
Žlutá	3	Vypnutý firewall	Nepravděpodobné	Střední

Tabulka 2 – Seznam zjištění

3 Soupis zjištění

Tato kapitola obsahuje seznam pozorování, která dle našeho názoru mají negativní dopad na bezpečnost a která jsou v rozporu se známými bezpečnostními politikami [Klienta] nebo s platnou legislativou („zjištění“). Vzhledem k tomu, že si nejsme vědomi, že by [Klient] deklaroval v bezpečnostní politice povinnost implementace jednotlivých CIS opatření, nepovažujeme za zjištění automaticky každý jednotlivý nesoulad s CIS.

3.1 Zjištění 1 Parametry hesel

3.1.1 Zjištění

Lokální nastavení serverů Windows 2008 R2 požaduje délku hesla alespoň 10 znaků. Na serverech Oracle Linux a v databázových serverech Oracle není nastaveno kontrolování délky ani komplexity hesla. Není zajištěna expirace hesel a není nastaveno zamykání systémů Oracle a Linux po neúspěšných pokusech o přihlášení. Na systému Windows je nastaveno zamykání po 15 špatných pokusech.

V databázích Oracle je ponecháno jednomu ze systémových uživatelů defaultní heslo.

3.1.2 Dopad

Není zajištěno, že parametry hesel jsou v souladu s požadavky vyhlášky o kybernetické bezpečnosti, která požaduje minimální délku hesla administrátorských účtů 15 znaků a změnu hesla po 90 dnech. Útočník mající přístup k serverům na síťové úrovni se může pokoušet o hádání hesel.

3.1.3 Doporučení

Doporučujeme zajistit technickými prostředky kvalitu hesel – v systémech Linux nastavením pravidel pam modulů, v systémech Windows doménovou politikou, v systémech Oracle prostřednictvím funkce testující kvalitu hesla – a zajistit změnu hesel všech defaultních účtů v existujících i nově konfigurovaných Oracle databázových serverech.

Vzhledem k očekávané změně požadavků vyhlášky na expirování hesel nepovažujeme nevynucované expirace hesel bod za prioritní.

3.2 Zjištění 2 Řízení práv uživatelů

3.2.1 Zjištění

Zejména na Windows serverech a v databázovém systému Oracle mají někteří uživatelé a role větší práva, než je by mělo být nezbytné.

Na systémech Windows se jedná o práva pro Everyone a Users pro přístup k serverům pro síť (mělo by postačovat Authenticated users), možnost běžných uživatelů se přihlašovat k serverům lokálně a práva uživatelů skupiny Guests.

Pro detaily nadbytečných práv v prostředí databází Oracle viz sekci 4 příslušného výstupu nástroje CIS-CAT. Lze očekávat, že část oprávnění může mít legitimní důvod, avšak zejména u oprávnění ponechaných v defaultním stavu toto nepředpokládáme.

3.2.2 Dopad

Oprávněný uživatel může provádět aktivity, které by mu měly být odepřeny. Zejména pro systémy Windows existují nástroje, které umožňují mapovat oprávnění uživatelů a hledat způsoby eskalace práv s jejich použitím až na úroveň administrátorů. Bez provedení takovéto analýzy nelze konkrétně dopad odhadnout.

3.2.3 Doporučení

Doporučujeme dodržovat princip minimálních oprávnění v serverovém prostředí.

3.3 Zjištění 3 Vypnutý firewall

3.3.1 Zjištění

Na serverech – jak Windows, tak Oracle Linux - je lokální firewall vypnut.

3.3.2 Dopad

V rámci lokální sítě není počítač chráněn před útoky na otevřené porty. To umožňuje útočníkovi s přístupem do vnitřní sítě získávat informace o serveru a potenciálně na ni provádět útoky.

Dopad zjištění je zmírněn tím, že síť je segmentována a servery jsou typicky v separátních podsítích, které jsou chráněny na úrovni síťových firewallů. Tím je dopad omezen na servery v jedné podsíti.

3.3.3 Doporučení

Doporučujeme zvážit vhodnost použití lokálních firewallů na serverech.

3.4 Zjištění 4 Defaultní konfigurace většiny bezpečnostních nastavení

3.4.1 Zjištění

Většina testovaných parametrů na Window serverech byla v registru ponechána v defaultním nastavení a nebyla definována doménovou politikou. Obdobně na Linuxových serverech a v Oracle databázích nebylo pozorováno provedení kroků běžně požadovaných v standardech pro hardening. To naznačuje, že hardening nebyl požadován.

Detailní seznam rozdílů, které pokládáme za významné, je v příloze A. Technické detaily jsou dále uvedeny v příložených výstupech CIS-CAT skriptů v příloze C.

Žádné z těchto zjištění samo o sobě neotvírá prostor pro útok. Jedná se typicky o chybějící vrstvy obranných mechanismů pro vícevrstvou obranu.

3.4.2 Dopad

V řadě parametrů systém není tak bezpečný, jak by mohl být. V dalších parametrech může lokální administrátor změnit nastavení lokálně i tam, kde to má negativní bezpečnostní dopad.

Dopad jednotlivých chybějících bezpečnostních nastavení a možnost je okamžitě uvést do souladu je různý a závisí na konkrétních okolnostech systému a komunikujících zařízeních.

3.4.3 Doporučení

Doporučujeme definovat způsob hardeningu (například odkazem na některý ze standardů s definováním výjimek), implementovat jej u nových systémů a dále provádět testování souladu existujících systémů s požadavky na hardening vhodným nástrojem.

4 Hodnocení rizik dle ZKB a VKB

Tato kapitola obsahuje hodnocení rizik souvisejících se zjištěními uvedenými v tomto dokumentu dle požadavků vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti (VKB), a dle kritérií stanovených v této vyhlášce.

4.1 Identifikované hrozby a jejich původci

Jako relevantní byly zvažovány následující hrozby a jejich původci.

	Hrozba	Původce	Hodnocení
3.	Kybernetický útok na systém s úmyslem získání osobních nebo jinak citlivých dat. Hrozbu hodnotíme jako střední, protože útočník musí mít základní povědomí o existenci systému, musí mít zájem na datech v systému, a tento způsob získání dat je pro něj jednodušší než alternativní možnosti.	Externí útočník, který má zájem a prostředky uskutečnit svoje hrozby	Střední
2.	Nezaměřený útok na zranitelné systémy (ransomware, viry, červi). Tyto útoky jsou běžně pozorovány v řádu několika významných za rok.	Útočník bez vztahu nebo povědomí o existenci [Klienta].	Vysoká
3.	Útok na systém z vnitřní sítě z pozice běžného uživatele s cílem získat oprávnění nad rámec přiřazených. Vzhledem k tomu, že takový útočník musí být ochoten podstoupit určité riziko a mít znalosti v oboru hodnotíme míru hrozby jako nízkou.	Zaměstnanec nebo kontraktor společnosti schopný provést útok na systém	Nízká

4.2 Klasifikace zjištění jako zranitelnosti

Zranitelnosti zjištěné během testu jsme v souladu s metodologií klasifikovali takto.

Zjištění	Hodnocení
Parametry hesel	Střední
Řízení práv uživatelů	Střední
Vypnutý firewall v lokální síti	Nízká (zejména z důvodu síťové segmentace)
Defaultní konfigurace většiny bezpečnostních nastavení	Střední
Absence detekčních mechanismů	Střední

4.3 Klasifikace dopadů

Možné dopady byly klasifikovány takto:

Popis	Dopad
Finanční pokuta za nedodržení ochrany osobních údajů za malý rozsah úniku dat (do 5 mil. CZK).	Nízký
Náhrada škod jednotkám klientů postižených únikem osobních dat. Předpokládáme, že výše vzniklé prokazatelné škody nebude více než 5 mil.	Nízký
Přerušení provozu uživatelů [Klienta] na krátkou dobu (do dvou dnů) a ztráta části neuložených dat uživatelů s dopadem na veřejnost od 251 do 2 500 osob a negativní celostátní publicitou do jednoho týdne.	Střední

4.4 Identifikovaná rizika

Na základě prověrky konfigurací jsme identifikovali a ohodnotili tato rizika. Hodnocení nebere do úvahy další možné kontroly, které mohou omezit hodnotu rizika, a v řadě parametrů je založeno na odhadu parametrů. Z tohoto důvodu doporučujeme revidovat ohodnocení odpovědnou osobou se znalostí vnitřního fungování [Klienta].

Popis rizika	Velikost hrozby	Závažnost zranitelnosti	Úroveň dopadu	Hodnota rizika
Externí útočník bez vztahu ke [Klientovi] vytvoří kód zaměřený na průnik do a šíření se v počítačích s konkrétními slabíny (typu nedávných útoků typu WannaCry apod.). Nezodpovědný uživatel zavleče škodlivý kód na jednotky zařízení v síti [Klienta] a z těch se nákaza rozšíří i na servery v síti. Tím dojde k narušení chodu společnosti, nutnosti reinstalovat nebo obnovit ze záloh servery, a ztrátě dat dosud nezazálohovaných. Vznikne škoda přerušením provozu s dopadem na veřejnost (do 2500 osob) a negativní publicitou.	Střední	Střední	Střední	Střední (1,5)
Interní uživatel (nebo třetí osoba s fyzickým přístupem k zařízením [Klienta]) s dostatečnými technickými znalostmi a odhodláním využije slabín systému (parametry hesel, absence lokálního firewallu, nadbytečná práva, jiná konfigurační nastavení), a získá přístup k a oprávněním která by neměla mít, nebo k přístupu bez patřičného logování. Toho využije k získání dat. [Klient] bude postižen za únik dat v malém rozsahu a negativní krátkodobé publicitou.	Nízká	Střední	Střední	Střední (1)
Externí útočník bez vztahu ke [Klientovi] vytvoří kód zaměřený na průnik do a šíření se v počítačích s konkrétními slabíny ve veřejně dostupných rozhraních (Apache http server, Tomcat). Částečný přístup s oprávněními příslušného serveru dokáže využít k eskalaci práv, získání dat nebo narušení služby. Dojde k postihu [Klienta] za toto narušení a krátkodobé negativní publicitou.	Střední	Nízká	Střední	

A Identifikované odchylky od požadavků standardu CIS

A.1 Windows 2008 R2

Servery tohoto typu měly vesměs téměř stejnou konfiguraci z hlediska souladu s CIS.

Detailní přehled odchylek od CIS je v příloze C. Zjištěné odchylky byly zapracovány takto:

- Parametry hesel:
 - o Doba platnosti hesla (90 dní) není v souladu s CIS, ale odpovídá politice a vyhlášce. Nevnímáme jako nesoulad.
 - o Minimální délka hesla 10 znaků je komentována ve zjištění Parametry hesel.
 - o Počet pokusů o zamčení hesla (15) je komentován ve zjištění Parametry hesel.
- Řízení práv uživatelů
 - o Obecně práva skupiny Backup Operators nevnímáme jako zjištění.
 - o Ve zjištění Řízení práv uživatelů komentujeme:
 - Přístup Everyone a Users k serverům po síti,
 - Možnost Users k lokálnímu přihlášení,
 - Práva „Guests“ k práci se systémem (2.2.18 až 2.2.21).
 - o Přejmenování účtů Administrators a Guests nepovažujeme za nezbytně užitečné opatření a dále nekomentujeme.
- Audit a logování
 - o Vzhledem k tomu, že z jiných projektů máme informaci o existenci a procesech logování a vyhodnocování logů, odchylky v této oblasti nekomentujeme.
- Správa zařízení
 - o Rozdíly oproti požadavkům CIS, kdy není nalezen očekávaný klíč, ale jeho absence vede k chování předepsanému CIS, komentujeme ve zjištění Defaultní konfigurace ... (2.3.4.1, 2.3.10.10, 2.3.11.3, 2.3.11.4).
- Síťový klient/server, Síťová bezpečnost
 - o Odchylku v těchto sekcích zahrnujeme do zjištění Defaultní konfigurace a považujeme za jednu ze závažnějších v tomto zjištění.
- Kontrola uživatelských účtů
 - o Odchylky 2.3.17.1, 2.3.17.3 jsou zahrnuty ve zjištění Defaultní konfigurace.
- Firewall
 - o Absence lokálního firewallu je komentována ve zjištění Vypnutý firewall.
- LAPS
 - o Absence používání LAPS není sama o sobě bezpečnostním zjištěním a není dále komentována, avšak používání nástroje pro správu administrátorských hesel je doporučeníhodné.

- MSS, nastavení sítě
 - o Odchyly v nastavení síťové vrstvy jsou obecně zahrnuty ve zjištění Defaultní konfigurace.
 - o Odchyly 18.4.11.3 je zahrnuta ve zjištění Defaultní konfigurace.
 - o Odchyly sekce 18.6 jsou zahrnuty ve zjištění Defaultní konfigurace.
- Systém
 - o Odchyly 18.8.19.2 a 18.8.19.3 jsou komentovány ve zjištění Defaultní konfigurace.
- Politiky pro Autoplay
 - o Odchyly v pravidlech pro automatické přehrávání považujeme za obtížně využitelné z důvodu nedostupnosti serverů kromě oprávněných osob a dále nekomentujeme.
- EMET
 - o Absenci nástroje EMET nekomentujeme zejména z důvodu očekávaného ukončení životnosti.
- Služby vzdáleného připojení
 - o Odchyly v nastavení služeb vzdáleného připojení jsou zahrnuty ve zjištění Defaultní konfigurace.

Ostatní zjištění nepovažujeme za nezbytné řešit. Formálně rovněž spadají pod zjištění Defaultní konfigurace.

A.2 Oracle Linux

Servery tohoto typu měly vesměs téměř stejnou konfiguraci z hlediska souladu s CIS.

Detailní přehled odchylek od CIS je v příloze C. Zjištěné odchylky byly zapracovány takto:

- Povolené nepoužívané filesystemy a absence nastavení mountování na virtuálních filesystemech dle našeho názoru s sebou nenesou využitelné riziko a byly zahrnuty do zjištění Defaultní konfigurace.
- Absence kontroly integrity filesystemu je komentována v sekci Defaultní konfigurace.
- Chybějící ochrany serverů při startu (heslo pro boot, ...) zahrnujeme do zjištění Defaultní konfigurace.
- Zjištění ohledně nastavení ssh rovněž zahrnujeme do zjištění Defaultní konfigurace.
- Nastavení parametrů hesel (neomezená expirace, minimální doba mezi změnami 1 den, chybějící zajištění požadavků na komplexitu, minimální délka) je komentováno ve zjištění Parametry hesel.
- Nastavování tcpwrappers považujeme v současné době za zastaralé a nepovažujeme za zjištění.
- Odchyly v nastavení firewallu komentujeme v sekci Vypnutý lokální firewall.

Ostatní odchylky nepovažujeme za nezbytné řešit a jsou zahrnuta obecně ve zjištění Defaultní konfigurace.

A.3 Oracle databáze

Servery tohoto typu měly vesměs téměř stejnou konfiguraci z hlediska souladu s CIS.

Detailní přehled odchylek od CIS je v příloze C. Zjištěné odchylky byly zapracovány takto:

- ponechané defaultní heslo je komentováno v sekci Parametry hesel.
- Odchylku v nastaveních LOCAL_LISTENER a REMOTE_LISTENER po zkušenostech s RAC konfiguracemi na jiných serverech považujeme za falešné pozitivum. Ověření odolnosti vůči TNS poisoning útoku může být provedeno nezávisle.
- Nastavení parametrů hesel – chybějící kontrola kvality hesla pro všechny uživatele, uživatele bez expirace a podobně – diskutujeme v sekci Parametry hesel.
- Vzhledem k tomu, že z jiných projektů máme informaci o existenci a procesech logování a vyhodnocování logů odchylky v této oblasti nekomentujeme.
- Většinu dalších odchylek komentujeme ve zjištěních Řízení práv uživatelů a Defaultní konfigurace.

A.4 Webové servery Apache

Servery tohoto typu měly opět vesměs téměř stejnou konfiguraci z hlediska souladu s CIS. Prověrka zde probíhala formou manuálního prověření konfigurace z vybraných serverů a není k dispozici strojový výpis výsledků.

Část požadavků CIS-CAT týkající se přístupových oprávnění k souborům a adresářům a nebyla kontrolována z důvodu neadekvátnosti předpokladu o operačním systému.

Vzhledem k tomu, že SSL je ukončováno na předřazených serverech, nebyly kontrolovány požadavky na SSL zabezpečení.

Obecně lze u webového serveru konstatovat relativně vysoký stupeň souladu s bezpečnostními požadavky CIS úroveň 1, v řadě případů byly implementovány i opatření CIS úrovně 2.

Byly zjištěny tyto odchylky od požadavků CIS úrovně 1:

- (2.4) Pro server b2bout je zaveden modul status_modul a není chráněn prostřednictvím kontroly IP adresy.
- (2.5) Je zaveden modul autoindex_module.
- (5.2) Nastavení práv (Options) k webové hierarchii neodpovídá požadavkům CIS (Options None).
- (5.7) Nejsou omezeny metody http requestů direktivou <LimitExcept>.
- (5.9) Není omezen přístup klientům používajícím HTTP/1.0.
- (5.10) Není omezen přístup k souborům .htaccess.
- (6.1) Do ErrorLog souboru se logují pouze varování, nikoliv level „info“. Na úrovni „info“ jsou logovány zejména „not found“ záznamy, které mohou pomoci detekovat pokusy o útok.

Tato zjištění považujeme za minoritní bez přímého dopadu na bezpečnost služby a spadají do kategorie Defaultní konfigurace.

A.5 Apache Tomcat

Servery tohoto typu měly opět vesměs téměř stejnou konfiguraci z hlediska souladu s CIS. Prověrka zde probíhala formou manuálního prověření konfigurace z vybraných serverů a není k dispozici strojový výpis výsledků.

Část požadavků CIS-CAT týkající se přístupových oprávnění k souborům a adresářům a nebyla kontrolována.

Opatření CIS týkající se způsobu spouštění nebyla kontrolována vzhledem k tomu, že startovací skript nebyl předán.

Obecně lze u webového serveru konstatovat relativně vysoký stupeň souladu s bezpečnostními požadavky CIS úroveň 1.

Byly zjištěny tyto odchylky od požadavků CIS úrovně 1:

- (2.5) Není zajištěno na úrovni konfigurace Tomcat, že uživatelé neuvidí v případě chyby detailní popis chyby včetně stack trace. Toto může být ošetřeno pro velkou část chyb přímo v aplikaci.
- (3.1) Není změněn příkaz pro shutdown port. Kdokoliv se síťovým přístupem tak může server vypnout. Na serverech t-portal01-XX je tato odchylka bez dopadu vzhledem k tomu, že shutdown port jako takový je vypnut (což je opatření CIS úrovně 2, které jsme jinak nehodnotili).

Tato zjištění považujeme za minoritní bez přímého dopadu na bezpečnost služby a spadají do kategorie Defaultní konfigurace.

B Postup analýzy rizik

V této sekci popisujeme obecný postup použitý v analýze rizik uvedené v kapitole 4 *Hodnocení rizik dle ZKB a VKB*.

B.1 Identifikace hrozeb

V analýze rizik byly v souladu s § 4 odstavcem (4) Vyhlášky zvažovány následující hrozby:

13. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
14. poškození nebo selhání technického anebo programového vybavení,
15. zneužití identity fyzické osoby,
16. užívání programového vybavení v rozporu s licenčními podmínkami,
17. kybernetický útok z komunikační sítě,
18. škodlivý kód (například viry, spyware, trojské koně),
19. nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,
20. narušení fyzické bezpečnosti,
21. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
22. zneužití nebo neoprávněná modifikace údajů,
23. trvale působící hrozby,
24. odcizení nebo poškození aktiva.

Hrozby byly v rámci analýzy rizik hodnoceny podle kritérií uvedených v příloze č. 2 k Vyhlášce.

Pro hodnocení hrozeb byla použita následující stupnice:

Koeficient	Úroveň	Popis
10%	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
30%	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
200%	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
1200%	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

B.2 Hodnocení zranitelností

Zranitelnosti byly v rámci analýzy rizik hodnoceny podle kritérií uvedených v příloze č. 2 k Vyhlášce. Pro jejich klasifikaci byla použita stupnice dle vyhlášky:

Stupnice pro hodnocení zranitelností

Koeficient	Úroveň	Popis
0	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, která jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
0,5	Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
0,7	Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
1,0	Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

B.3 Hodnocení dopadů

Pro hodnocení dopadů byla použita následující matice založená na příloze č. 2 k Vyhlášce.

Matice pro hodnocení dopadů

Oblast	Nízký (1)	Střední (10)	Vysoký (100)	Kritický (1000)
Dopad na hospodaření [Klienta]	Finanční nebo materiální ztráty do 5 000 000 Kč	Finanční nebo materiální ztráty od 5 000 000 Kč do 50 000 000 Kč	Finanční nebo materiální ztráty od 50 000 000 Kč do 500 000 000 Kč	Finanční nebo materiální ztráty převyšující 500 000 000 Kč
Dopad na veřejnost	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2 500 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2 501 do 25 000 osob	Dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25 000 osob
Finanční dopad na vedení [Klienta]	Finanční postih člena vedení ve výši do 50 tis. Kč	Finanční postih člena vedení ve výši od 50 do 200 tis. Kč	Finanční postih člena vedení vyšší než 200 tis. Kč	
Personální dopady na vedení [Klienta]	Disciplinární řízení	Odvolační z funkce, vedení trestního řízení	Zákaz výkonu povolání, trest odnětí svobody až do 3 let	Odvolační celého vedení [Klienta]
Nefinanční dopady	Negativní publicita v médiích s dosahem do 100 tis. obyvatel trvající méně než 1 týden	Negativní publicita v médiích s dosahem do 100 tis. obyvatel trvající více jak 1 týden	Negativní celostátní publicita trvající 1 měsíc	
	Negativní celostátní publicita trvající 1 den	Negativní celostátní publicita trvající do 1 týdne	Otevření diskuse o zrušení či výrazném omezení funkce [Klienta]	Zrušení či výrazné omezení funkce [Klienta]

B.4 Stanovení matice hodnocení rizik

Dopady byly v rámci analýzy rizik oceňovány podle kritérií uvedených v příloze č. 2 k vyhlášce 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Vzhledem k tomu, že jsme neměli k dispozici platnou metodiku [Klienta] pro analýzu a hodnocení rizik jsme na základě běžně používané praxe definovali metodiku takto:

Pro ocenění rizik byly stanoveny následující 4 úrovně rizik.

Název úrovně rizika		Naléhavost a intenzita reakce	Hodnota výše rizika		Barevné označení
5.	Malé riziko	Je nutné pouze registrovat a sledovat, zda se nezvyšuje	0-1		
6.	Střední riziko	Vyžaduje soustavnou pozornost a postupné zavádění opatření na jejich eliminaci	1-10		
7.	Velmi vysoké riziko	Vyžaduje okamžité zahájení plánování opatření na eliminaci rizika a alokaci potřebných zdrojů.	10-100		
8.	Kritické riziko	Vyžaduje neodkladné řešení, zapojení všech disponibilních zdrojů a zapojení vyššího vedení	100+		

Rizika jsou klasifikována na základě síly hrozby, stupně zranitelnosti a velikosti dopadu jako $\min(100, h \times z) / 100 \times d$, tedy takto:

- je odhadnuta roční pravděpodobnost využití příslušné hrozby daným aktivem vynásobením pravděpodobnosti hrozby (viz stupnici hrozeb) a koeficientem závažnosti slabiny (viz stupnici slabin),
- výsledek je omezen na maximálně 100%,
- tato pravděpodobnost vynásobená koeficientem velikosti dopadu určuje hodnotu rizika, podle které je zařazeno do úrovně.

Pro názornost uvádíme mapování získané pravděpodobnosti a dopadu na velikost rizika graficky; v posledním sloupci je uvedeno, jakou maximální pravděpodobnost může dosáhnout hrozba o dané síle (při kritické zranitelnosti).

Dopad	Nízký	Střední	Vysoký	Kritický	Maximum pro hrozby (kritická zranitelnost)
Pravděpodobnost					
pod 0.1%					
0.1% až 1%				Střední	
1% až 10%			Střední		Nízká
10% až 100%		Střední		Kritické	Střední
100%	Střední		Kritické	Kritické	Vysoká, Kritická

C Výstupy skriptů CIS-CAT a detailní seznam systémů

Výstupy nástroje CIS-CAT, na základě kterých bylo provedeno hodnocení pro systémy Windows Server, Oracle Linux a Oracle databáze, jsou ve vloženém souboru.

<soubor odstraněn>

Archiv obsahuje výstup z těchto serverů:

Microsoft Windows Server 2008 R2:

<odstraněno>

Oracle Database 12c:

<odstraněno>

Oracle Linux:

<odstraněno>

Kromě toho jsme vycházeli ze společností ACE předaných konfigurací Apache Web serveru a Apache Tomcat z dále uvedených serverů; tyto konfigurace nejsou součástí zprávy:

Tomcat:

<odstraněno>

V souladu s auditním plánem byly manuálně prověřovány zejména konfigurace portal01-xx, aud01-xx a sec01-xx.

Apache Web server:

<odstraněno>

V souladu s auditním plánem byly manuálně prověřovány zejména konfigurace <odstraněno>.



4. Povinnosti Poskytovatele

Poskytovatel se zavazuje po celou dobu trvání Smlouvy plnit Předmět plnění v souladu a alespoň ve stejné nebo vyšší kvalitě popisů penetračních testů a bezpečnostní prověrky uvedených v člancích 2. a 3. této Přílohy č. 1 této Smlouvy a poskytovat Objednateli součinnost alespoň v rozsahu uvedeném v článku 6. této Přílohy č. 1 této Smlouvy.

5. Součinnost ze strany Objednatele

Pro potřeby koordinace činnosti a poskytování odpovídajících informací bude na straně Objednatele ustanovena kontaktní osoba, která bude za spolupráci s dodavatelem odpovědná. S kontaktní osobou je Poskytovatel povinen v potřebném rozsahu spolupracovat a s touto osobou upřesnit všechny detaily spojené s obsahem a způsobem realizace Předmětu plnění. Tato osoba bude zajišťovat konzultace a zpřístupnění informací a dokumentů, které jsou pro provádění jednotlivých částí Předmětu plnění nezbytné.

6. Součinnost ze strany Poskytovatele

Pro potřeby koordinace činnosti a poskytování odpovídajících informací bude na straně Poskytovatele ustanovena kontaktní osoba, která bude odpovědná za spolupráci s Objednatelem a která bude v potřebném rozsahu spolupracovat s kontaktní osobou Objednatele, a to minimálně v na:

- přípravě plánů penetračních testů resp. bezpečnostních prověrek;
- přípravě autorizačních dopisů;
- zprostředkovávání doplňujících či vysvětlujících informací a dokumentů;
- informování o způsobu a parametrech provádění penetračních testů resp. bezpečnostních prověrek (např. konkrétní IP adresy, z nichž bude přistupováno do prvků IIS ČSSZ).

Detailní součinnost Poskytovatele bude pro plnění Dílčí smlouvy vždy odsouhlasena prostřednictvím autorizačního dopisu.

**Specifikace ceny Předmětu plnění**

Poskytovatel se zavazuje poskytovat Objednateli Předmět plnění dle této Smlouvy za ceny uvedené v následujícím přehledu:

Počet člověkohodin	Cena v Kč (bez DPH)	Cena v Kč (vč. DPH 21 %)
1 člověkohodina poskytování Předmětu plnění	830	1 004,30
4 900 člověkohodin poskytování Předmětu plnění	4 067 000	4 921 070

Výše uvedený počet 4 900 člověkohodin je pro tuto Smlouvu maximální a nepřekročitelný a Objednatel není povinen tento počet člověkohodin za dobu trvání této Smlouvy zcela vyčerpat. Objednatel tedy není povinen uhradit Poskytovateli za poskytování Předmětu plnění dle této Smlouvy celkovou maximální Cenu Předmětu plnění, nýbrž pouze cenu za skutečně poskytnutý Předmět plnění v podobě počtu člověkohodin strávených pracovníky Poskytovatele poskytováním Předmětu plnění. Člověkohodinou se rozumí 60 minut práce jednoho člověka skutečně provedené na plnění Předmětu plnění.

Výkaz plnění - vzor

(k Rámcové dohodě na zajištění penetračních testů a bezpečnostních prověrek integrovaného informačního systému ČSSZ s obchodní společností KPMG Česká republika, s.r.o.)

Výkaz za období.....

Příloha k faktuře č.

ID	Služba	Člověkohodiny (ČH)			Cena celkem (bez DPH)	Cena celkem (vč. DPH 21%)
		Počet ČH	Cena za 1 ČH (bez DPH)	Cena za 1 ČH (vč. DPH 21% DPH)		
A	Externí penetrační testování - prvotní externí penetrační testování	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
B	Externí penetrační testování - následné externí penetrační testování	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
C	Interní penetrační testování - prvotní interní penetrační testování	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
D	Interní penetrační testování - následné interní penetrační testování	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
E	Bezpečnostní prověrka infrastruktury IIS ČSSZ	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
F	Vyhotovení Závěrečné zprávy	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
G	Konzultační činnost Bezpečnostního specialisty k Závěrečné zprávě	[doplní Poskytovatel dle skutečně odpracovaných hodin]	830 Kč	1 004,30 Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč
Celkem:		[doplní Poskytovatel dle skutečně odpracovaných hodin, max. dle Dílčí	x	x	[doplní Poskytovatel dle Přílohy č. 2] Kč	[doplní Poskytovatel dle Přílohy č. 2] Kč



	smlouvy]				
--	----------	--	--	--	--

Za Poskytovatele KPMG Česká republika, s.r.o.:

Jméno a příjmení:

Podpis:

V Praze dne:

Za Objednatele Českou Republiku – Českou správu sociálního zabezpečení akceptoval:

Jméno a příjmení: [REDACTED]

Podpis:

V Praze dne:

Seznam aktuálně platných standardů IKT Objednatele

Číslo	Název standardu	Název dokumentu	Verze
1.	std_db_20151113_v0.97.doc	Standard databází	0.97
2.	std_inet_1_12.doc	Standard připojení k Internetu	1.12
3.	std_pošta_1_01.pdf	Standard poštovního systému ČSSZ	1.01
4.	std_AD_DNS_DHCP_NTP_2.05.pdf	Standard AD DNS DHCP	2.05
5.	std_AVO1_11.doc	Standard Antivirové ochrany	1.11
6.	Standard systémové konfigur. pracovní stanice 2.20	Standard systémové konfigurace pracovní stanice	2.20
7.	Std_mgmt_v.0.54.doc	Standard Management	0.54
8.	std_metodikavyvoje_apv_1_0_20.pdf	Standard metodiky vývoje	1_0_20
9.	std_pravidlareleasemanagementu_apv_1_2_7.pdf	Standard Release managementu	1_2_7
10.	std_net_1-95.docx	Standard síťové infrastruktury	1.95
11.	Programátorské konvence .NET 2.0 - 4.5_v1_0_19.pdf	Programátorské konvence .NET	1_0_19
12.	BizTalkDevelopmentStandard.v2.01.pdf	Standard pro tvorbu aplikací pro Microsoft BizTalk server	2.01
13.	AAA_Pozadavky_na_aplikace_v9.02	Požadavky na nové aplikace při integraci do AAA portálu	9.02
14.	Standard_pro_tvorbu_skriptu_db_Oracle_0.4.pdf	Standard pro tvorbu, předávání a spouštění skriptů v databázích Oracle	0.4
15.	Standard API rozhraní systému DMA - CSSZ_DMS_WS_API_DMA_v3_6.pdf	API ROZHRANÍ SYSTÉMU DMA: WS_API_DMA - Standard rozhraní pro ukládání dokumentů do DMS	3.6
16.	CSSZ_DU_STD_V_1.12.doc	Standard provozu databáze Oracle	1.12
17.	std_srv_0.41.doc	Standard systémové konfigurace aplikačních serverů verze	0.41
18.	std_PKI_v2.pdf	Standard pro PKI	2.0
19.	Standard Komunikace SD s exter firm v1_00	Standard komunikace Servicedesku s externími firmami	1.00
S6.1.	Standard Připravenost IIS ČSSZ na otevřená data.pdf	Standard Připravenost IIS ČSSZ na otevřená data	0.4
S6.2.	Standard Tvorba IRI RDF zdrojů.pdf	Standard Tvorba IRI RDF zdrojů	0.2
S6.3.	Standard Využívání KE.pdf	Standard využívání kmenových evidencí	0.4
S6.4.	Standard Využívání datového katalogu.pdf	Standard využívání datového katalogu	0.4
S6.5.	Standard Číselníky ČSSZ.pdf	Standard Číselníky ČSSZ	0.5



Příloha č. 5

Přehled poddodavatelů

Počet poddodavatelů = 0.

**Realizační tým Poskytovatele**

		Pozice: Bezpečnostní specialista
		Délka praxe: min. 5 let praxe v oblasti bezpečnosti informačních a komunikačních technologií
		Certifikace: ANO
		Certifikát: CISA
		Pozice: Člen bezpečnostního týmu
		Délka praxe: min. 3 roky praxe v oblasti informačních technologií
		Poddodavatel: NE
		Pozice: Člen bezpečnostního týmu
		Délka praxe: min. 3 roky praxe v oblasti informačních technologií
		Poddodavatel: NE
		Pozice: Člen bezpečnostního týmu
		Délka praxe: min. 3 roky praxe v oblasti informačních technologií
		Poddodavatel: NE

Poskytovatel uvede takový počet buněk tabulky výše, kolik je členů realizačního týmu Poskytovatele, minimálně však 3 osoby.

Podrobný popis způsobů uzavírání Dílčích smluv

Postup Smluvních stran

1. V souladu se Smlouvou, jejíž přílohou je tento dokument, se Smluvní strany zavazují provádět jakékoliv dílčí plnění Předmětu plnění dle Smlouvy výhradně na základě Dílčích smluv uzavřených v souladu a na základě objednávek (výzev) Objednatele uzavíraných způsobem blíže specifikovaným níže a dále v článku IV. Smlouvy.
2. Pojmy s počátečním velkým písmenem mají stejný význam, jako ve Smlouvě, není-li výslovně uvedeno jinak.
3. Pro zamezení pochybnostem Objednatel není povinen uzavřít žádnou Dílčí smlouvu a je oprávněn jednat o jejím uzavření kdykoliv ukončit a to i bez udání důvodu.

Způsob uzavírání Dílčích smluv

1. Objednatel zašle Poskytovateli výzvu k uzavření Dílčí smlouvy včetně písemného návrhu Dílčí smlouvy v souladu a v termínu dle článku IV. Smlouvy, a uvede případně další relevantní skutečnosti, s nimiž by měl být Poskytovatel seznámen před zahájením poskytování plnění na základě Dílčí smlouvy.
2. Poskytovatel je povinen návrh Dílčí smlouvy dle tohoto článku této Přílohy č. 7 do 10 (slovy: deseti) pracovních dnů od odeslání Objednatelům písemně potvrdit, nebo v případě, že Poskytovatel s návrhem nesouhlasí, je povinen ve stejné lhůtě doručit Objednateli svůj nesouhlas spolu s jím vypracovaným oponentním návrhem Dílčí smlouvy (v rozsahu počtu člověkohodin či termínu plnění). Za potvrzení návrhu Objednatele se považuje doručení podepsaného návrhu Dílčí smlouvy Poskytovatelem Objednateli. V případě, že Poskytovatel návrh nepotvrdí, ani neprojeví svůj nesouhlas dle tohoto článku tohoto odstavce Přílohy č. 7, platí, že návrh přijímá.
3. Objednatel na základě nesouhlasu Poskytovatele s návrhem posoudí Poskytovatelův oponentní návrh, přičemž při svém rozhodování může přihlídnout k obvyklé praxi v podobných případech; Objednatel doručí Poskytovateli reakci na oponentní návrh a Poskytovatel je povinen ve lhůtě dle odstavce 2 tohoto článku této Přílohy č. 7 doručit Objednateli přijetí reakce nebo nesouhlas. Protinávrh Objednatele na nesouhlas Poskytovatele se zněním reakce je závazný pro obě Smluvní strany. Objednatel bezodkladně po uzavření Dílčí smlouvy zašle Poskytovateli vyplněný a podepsaný Autorizační dopis, v němž Objednatel vyplní části uvedené v Příloze č. 8 vyznačené k doplnění Objednatelům.
4. Poskytovatel zašle Objednateli alespoň 4 (slovy: čtyři) pracovní dny před zahájením plnění dle Dílčí smlouvy vyplněný Autorizační dopis, v němž Poskytovatel vyplní části uvedené v Příloze č. 8 vyznačené k doplnění Poskytovatelem a podepíše jej, přičemž nebude provádět změny v Autorizačním dopise v částech vyplněných Objednatelům. Obsah Autorizačního dopisu lze před zahájením plnění na základě dohody Smluvních stran změnit, nikoliv však v rozporu s Dílčí smlouvou a takto také nelze změnit Dílčí smlouvu. V případě rozporů v obsahu Autorizačního dopisu má přednost obsah vyplněný Objednatelům.
5. Návrh, oponentní návrh, protinávrh, reakce, nesouhlas, Autorizační dopis, včetně dalších informací, výkazů, souhlasů či rozhodnutí dle tohoto článku této Přílohy č. 7, bude Smluvním stranám zasílán písemně na adresu uvedenou v záhlaví Smlouvy k rukám osoby oprávněné jednat ve věcech smluvních za konkrétní Smluvní stranu vlastnoručně podepsaný osobou oprávněnou jednat ve věcech smluvních za druhou Smluvní stranu.



6. Poskytovatel se zavazuje zahájit realizaci plnění Dílčí smlouvy neprodleně po uzavření Dílčí smlouvy na základě výzvy a návrhu Dílčí smlouvy dle tohoto článku této Přílohy č. 7, není-li v takové Dílčí smlouvě uzavřené postupem dle tohoto článku této Přílohy č. 7 stanoven jiný termín realizace.
7. Lhůty dle tohoto článku této Přílohy č. 7 lze po dohodě Smluvních stran prodloužit, a to zejména s ohledem na objektivní složitost požadovaného plnění v konkrétním případě, anebo pokud Poskytovateli brání v potvrzení návrhu vážné důvody, které není schopen objektivně překonat. Má-li prodloužení termínů dle tohoto odstavce tohoto článku této Přílohy č. 7 přímý vliv na jiné termíny uvedené ve Smlouvě či Příloze č. 7, prodlužují se takové termíny automaticky o dohodnutý počet dnů, a to pouze ve vztahu k Dílčí smlouvě, které se přímo týkají. V případě, k dohodě Smluvních stran dle první věty tohoto odstavce nedojde, platí termíny dle této Smlouvy.
8. Ustanovení článku IV. včetně článku VII. odst. 4 Smlouvy týkající se objednávky Objednatele a dalších jednání dle článku 1 této Přílohy č. 7 se na návrh Dílčí smlouvy a reakci na oponentní návrh dle tohoto článku této Přílohy č. 7 vztahují obdobně.



Vzor Autorizačního dopisu

Pro [Jméno a příjmení – doplní Objednatel]
[Pozice – doplní Objednatel]
Objednatel Datum [dd.mm.rrrr – doplní
Objednatel]

Od [Jméno a příjmení – doplní Poskytovatel]
[Pozice – doplní Poskytovatel]
Poskytovatel

Věc **Autorizační dopis k Provedení penetračních testů [Okruh – doplní
Objednatel] dle testovací metodiky OWASP Testing Guide v4**

Vážená paní, vážený pane

níže předkládáme Autorizační dopis k **Provedení penetračních testů [Okruh – doplní Objednatel] dle testovací metodiky OWASP Testing Guide v4** specifikující podmínky (pokyny Objednatele), za nichž budou provedeny uvedené penetrační testy.

Provedení penetračních testů [Okruh – doplní Objednatel] dle testovací metodiky OWASP Testing Guide v4 je realizováno jako plnění **[Dílní smlouvy č. xx – doplní Objednatel]** uzavřené na základě Rámcové dohody na zajištění služeb pro penetrační testování a bezpečnostní prověrky infrastruktury prvků IIS ČSSZ ze dne dd.mm.rrrr (dále rovněž jen „**Smlouva**“).

Účel dokumentu

Účelem tohoto autorizačního dopisu je

- zrekapitulovat a doplnit podmínky a informace nutné k provedení penetračních testů;
- naplánovat a schválit podrobnosti ohledně zahájení testů;
- za strany Objednatele a Poskytovatele deklarovat:
 - připravenost pro spolupráci při plánování testu a přípravě testu (harmonogramu apod.);
 - asistenci technických pracovníků ČSSZ a spolupráci při ověřování existence a závažnosti zjištěných nedostatků;
- Ujednotit řízení a organizaci testů, zejména v oblastech:
 - zásady pro provádění testů;
 - plán testů;
 - zásady pro zvládání mimořádných situací;
 - komunikační matice pracovníků, kteří se podílejí na provádění testů.



Rozsah a cíl bezpečnostních testů

V souladu se Smlouvou a Dílčí smlouvy budou provedeny penetrační testy [Okruh – doplní Objednatel dle Dílčí smlouvy], a to dle testovací metodiky OWASP Testing Guide v4.

Cílem penetračních testů bude odhalení veškerých bezpečnostních slabín včetně související infrastruktury a návrh účinných opatření k jejich eliminaci včetně stanovení priorit při jejich realizaci.

Testovaná aplikace

- [bude doplněno Objednatelem v návaznosti na podmínky testování]

Přístupové údaje

Pro účely bezpečnostních testů bude použita ...[bude doplněno Objednatelem v návaznosti na podmínky testování]

Postup a způsob realizace

Bezpečnostní testy budou realizovány[bude doplněno Objednatelem v návaznosti na podmínky testování]

Metodika

Testy webové prezentace budou zaměřeny zejména na bezpečnostní slabiny definované v dokumentu OWASP Testing Guide v4.

Součástí všech testů bude zjištění slabín a analýza možností jejich využití k provedení konkrétních útoků (vulnerability assessment).

Prostředí a nastavení

- Testy proběhnou v [produkčním/testovacím – doplní Objednatel] prostředí.
- Testy budou prováděny z [doplnit místo – doplní Objednatel].
- Testy budou prováděny ze zařízení (osobních počítačů) pracovníků Poskytovatele.
- Testy budou prováděny z dedikované IP adresy [xxx.xxx.xx.xxx – doplní Poskytovatel].
- Testy budou realizovány dle potřeby následujícími zaměstnanci Poskytovatele, kteří jsou oprávněni provést bezpečnostní prověrku ve výše specifikovaném rozsahu:
 - [Jméno příjmení – doplní Poskytovatel]
 - [Jméno příjmení – doplní Poskytovatel]
 - ...

Plán testů – Harmonogram

- Ověření přístupnosti a připravenosti prostředí pro penetrační testy proběhne v rozmezí [od dd. do dd.mm.rrrr – doplní Poskytovatel dle Dílčí smlouvy].
- Realizace bezpečnostních testů proběhne v období [od dd. do dd.mm.rrrr – doplní Poskytovatel dle Dílčí smlouvy].



- Předběžná zpráva bude předložena [dd. dd. rrrr – doplní Poskytovatel dle Dílčí smlouvy], nestanoví-li Smlouva jinak.
- Návrh Závěrečné zprávy bude předán do [dd. dd. rrrr – doplní Poskytovatel dle Dílčí smlouvy], nestanoví-li Smlouva jinak.

Předané podklady

V rámci podkladů pro testování byly ze strany Objednatele předány následující podklady:

[název dokumentu – doplní Objednatel]

Zásady provádění testů

- Testování, jeho průběh a časování se bude řídit plánem testů.
- V průběhu testů nesmí být použity útoky typu DoS nebo DDoS.
- Během testů budou operativně ověřovány s Objednatelem zejména závažné nálezy testu tak, aby mohly být případně okamžitě odstraněny.

Potřebná součinnost Objednatele

- [bude doplněno Objednatelem v návaznosti na podmínky testování]

Komunikace v době přípravy a průběhu testů

- Osoba Objednatele odpovědná za věcné plnění a koordinátor Objednatele bude informován Poskytovatelem o zahájení jednotlivých částí testů a o jejich průběhu.
- Osoba Objednatele odpovědná za věcné plnění a koordinátor Objednatele bude informován Poskytovatelem o ukončení jednotlivých částí testů.
- Osoba Objednatele odpovědná za věcné plnění bude neprodleně informována Poskytovatelem o zjištěných kritických nedostacích již v průběhu testů.
- Formální závěry budou předány Poskytovatelem ve formě Závěrečné zprávy z bezpečnostního testování výhradně osobě odpovědné za věcné plnění Objednatele.

Slova či sousloví uvedená s počátečním velkým písmenem mají stejný význam, jako ve Smlouvě, jsou-li ve Smlouvě definována. V případě rozporu tohoto Autorizačního dopisu a Smlouvy mají přednost ustanovení Smlouvy.

Za Objednatele

Za Poskytovatele

.....

.....

Datum, podpis

Datum, podpis

